Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 10, October 2021: 2045-2058

SECURED AND RELIABLE DATA COMMUNICATION IN INTERNET OF THINGS

D.Balakrishnan [1] , T.Dhiliphan Rajkumar [2] , S.Dhanasekaran [3] , B.S.Murugan [4]

1 Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil-626126, Tamilnadu, India
2 Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil-626126, Tamilnadu, India
3 Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil-626126, Tamilnadu, India
4 Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil-626126, Tamilnadu, India
Email: 1 d.balakrishnancse@gmail.com, 2 t.dhiliphan@klu.ac.in, 3 srividhans@gmail.com, 4 b.s.murugan@klu.ac.in

ABSTRACT

Increased technologies prompts higher usage of the IoT devices which will in general perform information detecting and communication. Here got communication turns into the more prominent concern which would influence the legitimate and effective information communication. This is accomplished in the current exploration work by presenting the strategy specifically Elliptic Curve Cryptography (ECC) technique base validation where confirmation of entomb associated devices will be performed prior to permitting the information transmission. In the current work, there could be no legitimate technique followed for the proper dynamic with regards to the vindictive node presence. In the current work, it is referenced that the confirmation is acted in the firewall. Anyway verification system used in the current work is more conventional and it can't uphold high characterized applications. This is settled in the proposed work by presenting the strategy specifically Modified ECC based Authentication Framework (MECC). In this exploration work, point duplication based ECC strategy is used for the got information communication. New key age strategy is presented for the expanded security level by utilizing which encryption will be performed. To keep away from the malignant exercises verification is performed at the firewall. This verification is performed dependent on traffic stream. In firewall SVM calculation is executed for the appropriate dynamic with regards to the vindictive node presence. The general investigation of the exploration work is done in matlab climate from which it is demonstrated that the proposed techniques can will in general give better and got communication over the current devices.

Keywords: Elliptic curve cryptography, authentication, interconnected devices, modified ECC method, firewall SVM, new key generation

I. INTRODUCTION

The Internet of Things (IoT) addresses the interconnection, through the Internet, of an enormous number of 'Things' – interestingly recognizable actual items with detecting, communication and

activation abilities [1]. The term has been presented by Kevin Ashton in 1999 with regards to chain supply the board [2]. There are presently 5 billion brilliant items associated with the Internet, and it is normal that there will be 25 billion by 2020. The mix of 'Things' in the Internet is testing since they might have attributes like restricted memory, handling limit and energy assets [3]. Most items were at first evolved as shut exclusive arrangements that were incompatbile with devices from different merchants [4]. The latest thing anyway is towards normalized and interoperable protocols.

As the field of IoT extends, assaults against IoT frameworks are filling in number and intricacy [5]. Assaults against IoT frameworks mean to take touchy information, infuse false data or disturb the ordinary usefulness of organizations and administrations [6]. Late assaults took advantage of weaknesses in keen fridges, in clinical devices and keen vehicles [7]. A few assaults might imply significant danger, for instance, hacking clinical devices might prompt the deficiency of living souls. In this way guarantee the security of basic IoT frameworks by giving assurance against noxious assaults and disappointments [8].

By and large, data security manages classification, integrity and accessibility (CIA) [9]. Schneier states that in the Internet of Things, assaults against trustworthiness and accessibility are a higher priority than assaults against classification [10]. For instance, in a savvy home climate with a shrewd lock, keep an attacker from controlling the lock (to go into the house or square the entryway), than from discovering that somebody has gone into the house [11]. Likewise keep an assailant from controlling your vehicle, than from snoopping on your area. The fundamental test in IoT security is to keep assailants from acquiring command over the IoT framework [12].

Communication issue incorporates the choice of suitable protocols just as the plan of organization security framework to get the communication processes [13]. This turned into a necessity as the assault on the IoT framework became increasingly more alongside the improvement of IoT innovation itself. These assaults for the most part plan to take significant information, enter false information into the framework, or control the framework wrongfully undetected by the framework proprietor [14]. Such attacks are positively exceptionally risky and can cause enormous losss. For instance, in keen home framework case, these assaults can make a home available to non-proprietors and can prompt criminal demonstrations like theft. Notwithstanding communication issues, one more significant thing to note in the plan of IoT frameworks, particularly brilliant home framework, is information base plan. Information is an article conveyed between one component with different components in the framework. The innovation advancement of an IoT framework positively affects the more noteworthy measure of information which should be put away in the information stockpiling component. In this way, the plan of a conservative data set would be important to save extra room.

The principle commitment of this examination work is to present the methods which can perform protected communication between the IoT devices with guaranteed confirmation. This is finished by presenting the appropriate confirmation system which can prompts got information communication without interloper contribution. This is guaranteed by presenting the adjusted ECC protocol which can play out the suitable information communication. And afterward got communication is ensured by presenting the new key age technique which can guarantee the fitting and protected information

communication with expanded hacking intricacy. At long last gatecrasher contribution is tried not to by carry out the traffic examination based interloper presence recognition.

II. RELATED WORKS

Porkodi and Bhuvaneswari [15] distinguished the chances, issues, challenges and the innovation norms utilized in IoT like Radio-Frequency IDentification (RFID) labels, sensors, actuators, cell phones, and so on This work is of two overlay, the principal crease covers the various applications that took on shrewd advancements up until now. The second overlap of this work presents the outline of the sensors and its guidelines.

Fuller et al [16] presented in this a data concealing procedure for infusing maneuvered bundles toward remote sensor organizations (WSNs). Creators displayed how an attacker can apply data stowing away as a kind of secretive channel assault over radio recurrence transmissions into the WSN. The attainability of our infusion strategy is exhibited through an assault on the most widely recognized execution of the ITU-T G.9959 proposal, industrially known as Z-Wave. All the more explicitly, we represent that subsequent to getting to a Z-Wave door regulator through compromising the WLAN spine, the attacker can introduce malware. The malware checks approaching Z-Wave packets for data concealed in Media Access Control (MAC) outlines got by the Z-Wave regulator.

Hao [17] indicated a Password-Authenticated Key Exchange by Juggling (J-PAKE) protocol. This protocol permits the foundation of a solid start to finish communication channel between two remote gatherings over an unreliable organization exclusively dependent on a common secret key, without requiring a Public Key Infrastructure (PKI) or any confided in outsider.

Raza et al [18] introduced a 6LoWPAN/IPsec augmentation and show the feasibility of this methodology. Creators depicted the 6LoWPAN/IPsec execution, which is assessed and contrasted and the execution of IEEE 802.15.4 link-layer security. Creators likewise showed that it is feasible to reuse crypto equipment inside existing IEEE 802.15.4 handsets for 6LoWPAN/IPsec. The assessment results show that IPsec is an achievable choice for getting the IoT as far as packet size, energy utilization, memory use, and handling time.

Nir et al [19] replaces RFC 7321, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)". The objective of this work is to empower ESP and AH to profit from cryptography that is state-of-the-art while making IPsec interoperable.

Raza [20] empowered secure communication in the IoT utilizing lightweight packed at this point standard agreeable IPsec, DTLS, and IEEE 802.15.4 connection layer security; and it examines the upsides and downsides of every one of these arrangements. The proposed security arrangements are executed and assessed in an IoT arrangement on genuine equipment. This work additionally presents the plan, execution, and assessment of an original IDS for the IoT. To wrap things up, it additionally gives instruments to secure information inside compelled nodes. The exploratory assessment of the various arrangements shows that the asset obliged devices in the IoT can be gotten with IPsec, DTLS, and 802.15.4 security; can be effectively ensured against interruptions; and the proposed

consolidated secure stockpiling and communication systems can altogether decrease the security-related activities and energy utilization.

Raza et al [21] introduced Lithe-a joining of DTLS and CoAP for the IoT. With Lithe, creators moreover propose an original DTLS header pressure conspire that means to altogether lessen the energy utilization by utilizing the 6LoWPAN norm. Above all, our proposed DTLS header pressure plot doesn't think twice about start to finish security properties given by DTLS. At the same time, it significantly decreases the quantity of sent bytes while keeping up with DTLS standard consistence.

Fernandes et al [22] proposed Advanced Message Queuing Protocol (AMPQ). To assess the exhibition of this methodology, this paper presents a presentation correlation investigation of RESTful Web administrations and the AMQP Protocol considering trading messages among customer and server. The review depends on the found the middle value of traded messages for a while. It was noticed and presumed that, for huge amounts of messages trade, the best outcomes comes from the Advanced Message Queuing Protocol.

III. SECURED INTER DEVICE COMMUNICATION METHOD

In this exploration work, point increase based ECC strategy is used for the got information communication. New key age strategy is presented for the expanded security level by utilizing which encryption will be performed. To stay away from the malevolent exercises confirmation is performed at the firewall. This validation is performed dependent on traffic stream. In firewall SVM calculation is carried out for the legitimate dynamic with regards to the malevolent node presence.

3.1. NEW KEY GENERATION FOR INCREASED SECURITY LEVEL

In this stage, every node in climate will create their arbitrary number. This irregular number will be imparted to the bunch head for additional confirmation cycle. An irregular number generator (RNG) is a device that produces an arrangement of numbers or images that can't be sensibly anticipated better compared to by an arbitrary possibility. Arbitrary number generators can be valid equipment irregular number generators (HRNG), which produce really irregular numbers, or pseudo-irregular number generators (PRNG) which create numbers which look arbitrary, yet are really deterministic, and can be duplicated if the condition of the PRNG is known. Pseudo Random Number Generator (PRNG) alludes to a calculation that utilizes numerical equations to create arrangements of irregular numbers. PRNGs produce a succession of numbers approximating the properties of irregular numbers. A PRNG begins from a subjective beginning state utilizing a seed state. Many numbers are produced in a brief time frame and can likewise be imitated later, if the beginning stage in the arrangement is known. Thus, the numbers are deterministic and proficient. With the appearance of PCs, developers perceived the requirement for a method for bringing irregularity into a PC program. Nonetheless, amazing as it might appear, it is hard to get a PC to accomplish something by chance as PC adheres to the given directions aimlessly and is thusly totally unsurprising. It is preposterous to expect to create genuinely arbitrary numbers from deterministic thing like PCs so PRNG is a procedure created to produce irregular numbers utilizing a PC. Straight Congruential Generator is generally normal and most seasoned calculation for producing pseudo-randomized numbers. The generator is characterized by the repeat connection:

$$X_{n+1} = (aX_n + c) \bmod c$$

where X is the sequence of pseudo-random values

m, 0< m- modulus

a, 0< a <m- multiplier

c, 0< = c<m- increment

x_0, 0<=x_0<m- the seed or start value

We produce the following irregular whole number utilizing the past arbitrary whole number, the number constants, and the number modulus. To get everything rolling, the calculation requires an underlying Seed, which should be given by certain means. The presence of haphazardness is given by performing modulo number juggling.

Leave X alone either a symmetric key or the irregular worth to be utilized as contribution to a supported hilter kilter key pair age calculation. X will be a piece string worth of the accompanying structure:

$$X = U \oplus V$$

where

• U is a piece line of the ideal length that is gotten as the yield of an endorsed PRNG that is fit for supporting the ideal security strength needed to ensure the objective information,

• V is a piece line of a similar length as U, and

• The worth of not really set in stone in a way that is autonomous of the worth of U (as well as the other way around).

The calculation with which X will be utilized, and the security strength that this use is planned to help will decide the necessary digit length and additionally the base security strength that this cycle should give. Since there are no limitations on the determination of V (other than its length and its autonomy from U), a moderate methodology requires a supposition that the cycle used to choose U gives most (if not the entirety) of the necessary entropy. The freedom necessity on U and V is deciphered in a computational and a factual sense; that is, the calculation of U doesn't rely upon V, the calculation of V doesn't rely upon U, and knowing one of the qualities (U or V) should yield no data that can be utilized to acquire understanding into the other worth. Accepting that U is the yield of an endorsed PRNG, coming up next are instances of autonomously chose V qualities:

1. V is a steady (chose freely from the worth of U). (Note, that assuming V is a line of twofold zeroes, K = U, i.e., the yield of a supported PRNG.)

2. V is a key acquired utilizing a supported key-induction technique from a key deduction key and other information that is autonomous of U;

3. V is a key that was freely produced in another cryptographic module. V was secured utilizing a supported key-wrapping calculation or shipped utilizing an endorsed key vehicle conspire during resulting transport. Upon receipt, the security on V is eliminated inside the key-producing module that created U prior to joining V with U.

4. V is delivered by hashing one more piece string (V ′) utilizing a supported hash work and (if essential) shortening the outcome to the fitting length prior to joining it with U. That is, V = T(H(V ′), k) where T(x, k) signifies the truncation of touch string x to its k furthest left pieces, and k is the length of U. The piece string V ′ might be a) a consistent; b) a key got from a common mystery during an endorsed keyagreement conspire between the key-producing module and another cryptographic module; or c) a key that was I) autonomously created by another module, ii) sent utilizing a supported key wrapping calculation or moved utilizing an endorsed key vehicle plan, and iii) upon receipt, the insurance on the key was eliminated.

3.2. MODIFIED ELLIPTIC CURVE CRYPTOGRAPHY BASED SECURED DATA TRANSMISSION

Various equipment, programming items just as guidelines, which use public key technique for encryptions, decodings are reliant upon RSA cryptosystem. The increment in the key length could work on the security of the RSA cryptosystem; regardless it needs extra computational expense. This Additional expense contains results, especially for those trade destinations that complete safer exchanges. In the new year, a public key cryptosystem has demonstrated its capacity to dare RSA. This cryptosystem utilized here is Elliptic curve cryptosystem. The premier interest of ECC is that it could offer prevalent execution just as security for a far off more modest key size, when contrasted with RSA cryptosystem. This is the manner by which it diminished the computational expense or handling cost. When contrasted with RSA cryptosystem, the math of ECC is extremely composite.

3.2.1. MATHEMATICS OF ECC

Elliptic curves just as chart of the cubic curves is explained in this portion. Elliptic curves are cubic condition that is as per the following,

$$y2 = x3 + ax2 + bx + c \quad (1)$$

When an elliptic curve contains two points and draw a line between both of them, the line would overlap the curve on distinctive third point. According to equation (1) a, b, c are real numbers and x, y are real variable. The subsequent form is enough for our elucidation

$$y2 =x3 + ax + b \quad (2)$$

3.2.2. GRAPH OF THE CUBIC CURVE

Worth of y is created for each worth of x and furthermore for the decent worth of a, b. clearly, the elliptic curve for the situation (2) will be symmetric consistently about x node. In light of the worth of y is continually being even. Henceforth, the condition (2), in relationship with point O known as zero point or point at proclivity. The elliptic curve E(a,b) where a=-1 and b=o, the absolute focuses can be {(0,0),(1,0),(2,√6)… } that fulfills y2=x3-x. Figure 1(a) signifies the diagram of this cubic curve condition.

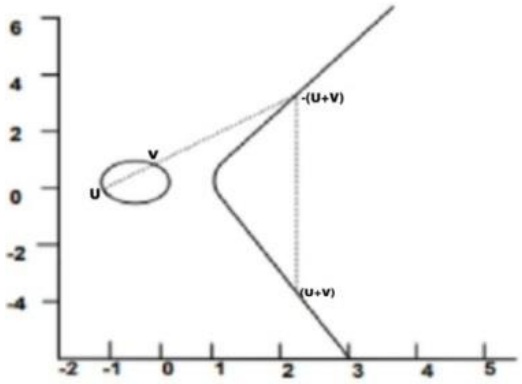

Figure 1.(a) Curve of y2=x3-x

Likewise, E (1, 1) represents the curve y2=x3+x+1.

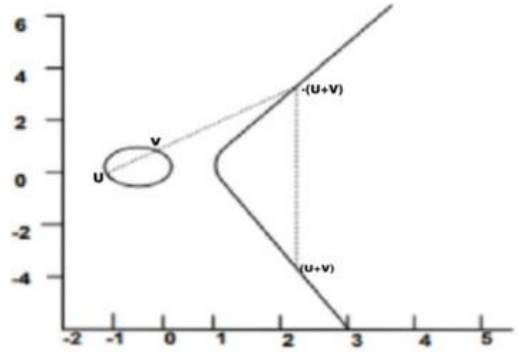

Figure 1: (b) curve of y2=x3+x+1

The point duplication should be possible quick utilizing both programming execution and equipment execution. The parallel technique, NAF strategy are the product implantation for point duplication. The k-NAF ECC processor is equipment design for doing point increase.

3.2.3. POINT MULTIPLICATION USING BINARY METHOD

The condition V=kU is utilized ordinarily for scalar point duplication in which U, V are elliptic curve focuses and k is a whole number. The worth of V is determined by monotonous expansion and multiplying procedure on focuses. For registering V, number k is signified as $k=k_{n-12n-1}+k_{n-22n-2}$ + . . . + k_1+k_0 in which kn-1=1 and k_i has a place with {0,1}, where I = 0 to n-1. This strategy is called as double technique. In twofold technique, examining is done from left to right or right to left for k pieces. The accompanying calculation portrays the calculation of k_V utilizing parallel technique.

Algorithm: Point Multiplication using Binary Method

Input : Binary representation of k and point V

Output : U = kV

U=V ; i=n-1;

While (i<0) do

U = 2U (Doubling)

If (k_i == 1) then

$$V = V + U \text{ (Addition)} \quad (3)$$

Return V

The temporal expense of duplication is straightforwardly relative to no. of 1s in the portrayal. The Hamming Weight of any scalar is the quantity of non-zero digits. Paired strategy needs (n-1) multiplying (ECDBL) and (n-1)/2 augmentations (ECADD). For each cycle '1', it should complete ECC serving just as ECC expansion, when the digit is '0', it requires essentially ECDBL activity. Accordingly, the quantity of 1s is getting lessened. This scalar portrayal is known as hamming weight. When hamming weight diminishes, then, at that point, scalar duplication is getting increments.

3.3. FIREWALL FILTERING BASED ON TRAFFIC ANALYSIS USING SUPPORT VECTOR MACHINE

Despite the fact that there is no think twice about what sort of traffic should be investigated as "unusual", the customary knowledge is that the traffic delivered by network assaults ordinarily shows some extraordinary elements. Like the heap estimations outlined over, a disseminated set of tests is used for include extraction. Portentously it doesn't focus on a singular arrangement of qualities anyway use a bunch of tests to take out attributes from an assortment of protocol layers. In this exploration technique burst time examples additionally considered alongside the circumstance genuine qualities (like sort of protocols, TTL esteems, geo-area of intelligent IPs, and so forth) In the proposed work, assault identification proportion is improved by presenting the AI methods to be specific Support Vector Machine which will get familiar with the assaults highlights in the ideal way. Backing vector machine (SVM) is a directed calculation and it is utilized for forecast reason in any given dataset. For Intrusion Detection System (IDS) boundaries forecast, we use SVM which is ideal isolating hyperplane between the two classes of information. SVM models used to deliver better forecast results.

Formula

Training dataset (D)

$D = \{x_i, y_i\}_{i=1}^{N}, \quad x \in R^n, y \in \{-1, 1\}$ (4)

D is training dataset, x and y is input variables

$y^i[|w^T x^i + b|] \geq 1 \quad i=1 \text{ to } N$ (5)

w^T and b are separated variables

To reduce the error minimization we can use given below formula

$\Phi(w) = \frac{1}{2}||w||^2$ (6)

Estimating function

$F(x) = \sum_{i=1}^{nsv}(x_i, y_i)k(x_i, y_i) + b$ (7)

SVM Algorithm Procedure

Given dataset D=(x1, y1),……,(xn, yn), C // x and y –labeled samples and C-class

Initialize vector v=0, b=0; class) // v-vector and b-bias

Train an initial SVM and learn the model

For each $x_i \in X$ do // xi is a vector containing features describing example i

Classify x_i using f (x_i)

If y_i f (x_i) < 1 // prediction class label

Find w', b' for known data // w', b' for new features

Add x_i to known data

Minimize the error function using (6) and estimate using (7)

If the prediction is wrong then retrain

Repeat

End

Classify attributes as normal or abnormal

IV. RESULTS AND DISCUSSION

In this segment, the matlab test system is utilized to assess the exhibition of the proposed MECC. The proposed framework MECC execution is assessed by contrasting it and the current framework

ECC. The presentation of MECC was assessed utilizing the accompanying measurements like packet loss, bundle conveyance proportion, energy utilization, false positive rate and false alert rate.

4.1. PACKET LOSS

The total number of information packets lost genuinely or through pernicious activity with no warning. Figure 2 shows the graphical portrayal of packet loss rate, it shows that the MECC technique has lower bundle loss rate when contrasted and the current frameworks ECC.

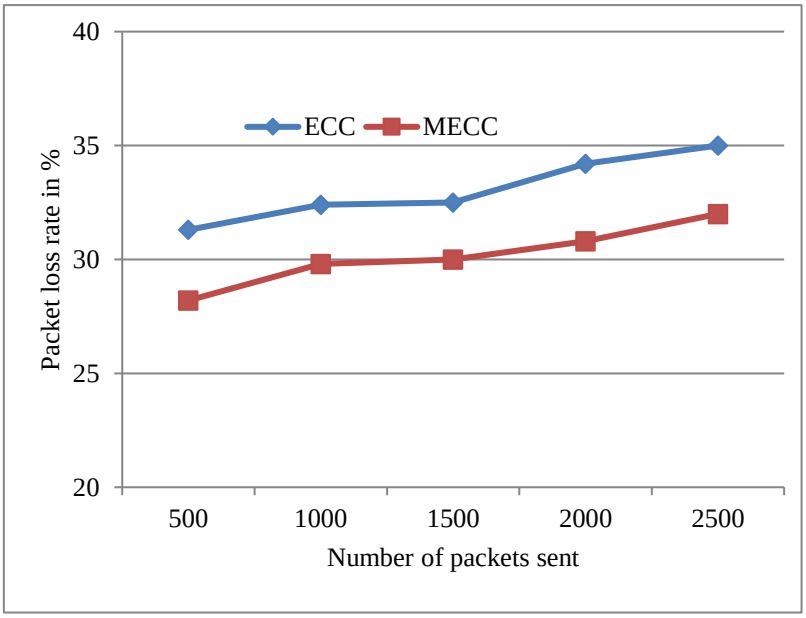

Figure 2 Comparison of packet loss in different trust model

The current framework doesn't zero in on contrast between the real nodes and the malignant as it considers each sensor node with high traffic deviation as the vindictive. The proposed calculation recognizes the individual noxious nodes dependent on inclination and fluctuation esteem accordingly the packet drop by the veritable nodes can be kept away from. The exploratory outcomes shows that proposed MECC have lesser packet loss rate when looked at existing ECC.

4.2. PACKET DELIVERY RATIO (PDR)

It is the proportion of the total number of information packets got to the complete number of information bundles communicated. This represents the degree of conveyed information to the objective.

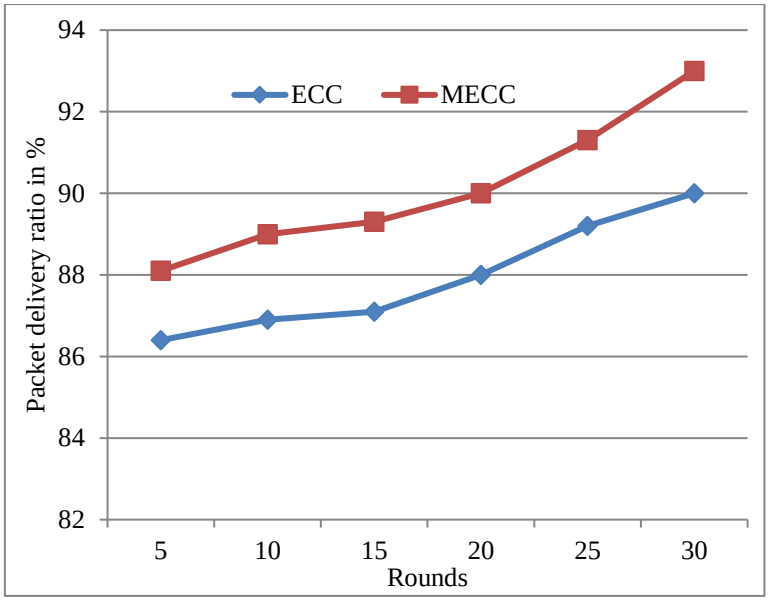

Figure 3 Comparison of packet delivery ratio for different trust system

Figure 3 shows the presentation of the proposed MECC contrasted with ECC with deference with the quantity of rounds and Packet Delivery Ratio (PDR). The quantity of packets which is successfully gotten at the objective without the deficiency of any bundles or disappointment for the proposed MECC is high which shows higher PDR results.

4.3. ENERGY CONSUMPTION

The normal energy devoured by every node during the given recreation time is communicated in Joules (J).

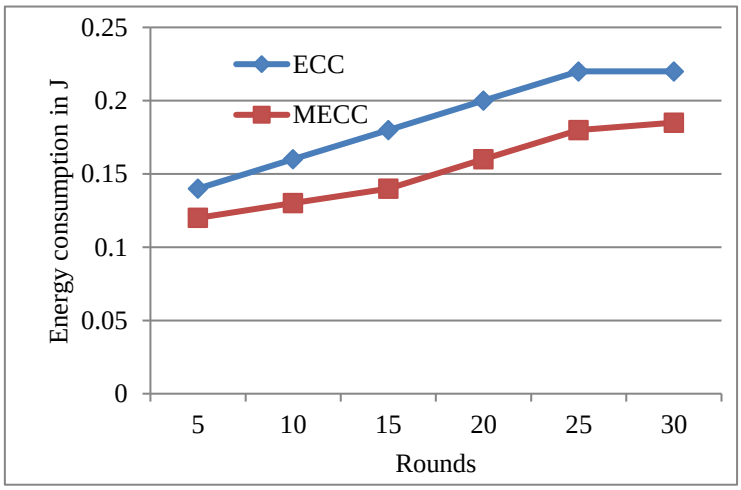

Figure 4 Comparison of energy consumption of different trust system

Figure 4 shows the graphical portrayal of energy utilization for various trust models in remote sensor organization of military applications. The MECC strategy has low energy utilization when contrasted and the current framework ECC.

4.4. FALSE ALARM RATE

A false alert proportion, by and large condensed FAR, is the quantity of false cautions per the total number of admonitions or cautions in Sybil assault discovery. In the accompanying figure false alert rate examination is displayed against various number of attacker nodes presence in the climate.

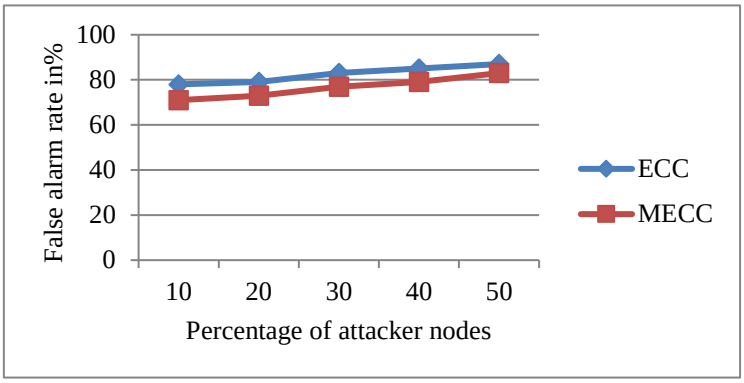

Figure 5. False alarm rate vs number of attacker nodes

In figure 5, correlation assessment of the false alert rate for the proposed and existing techniques are given. From this correlation it very well may be demonstrated that the proposed technique MECC will in general have preferable execution over the past philosophies with lesser wrong discovery of assailant nodes.

False positive rate

The false positive rate is determined as the proportion between the quantity of adverse occasions wrongly sorted as sure (false up-sides) and the total number of real adverse occasions (paying little heed to grouping). False positive rate, which is the rate that our calculation inaccurately recognizes the node.

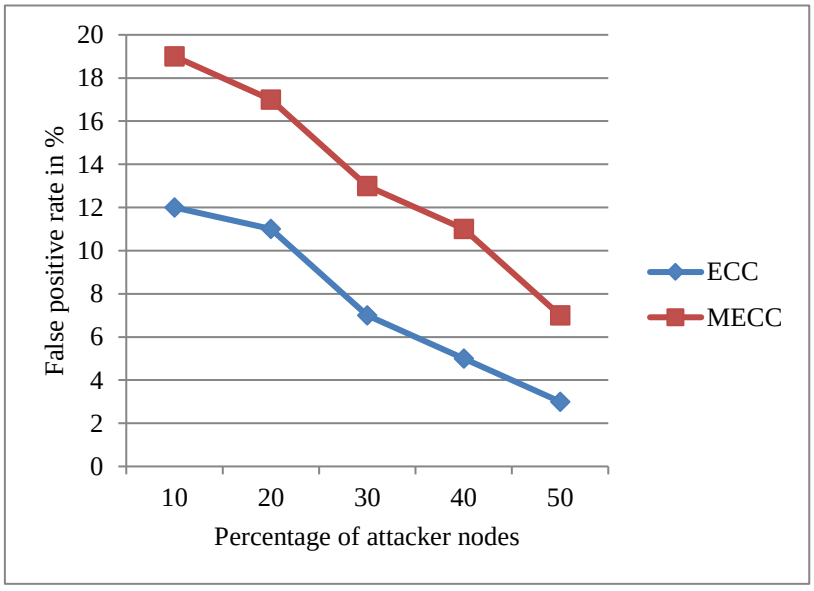

Figure 6. False positive rate vs percentage of attacker nodes

secured and reliable data communication in internet of things

In figure 6, correlation assessment of the false positive rate for the proposed and existing strategies is given. From this correlation it very well may be demonstrated that the proposed strategy MECC will in general have preferred execution over the past approaches with lesser wrong location of attacker nodes.

V. CONCLUSION

In this exploration work, point duplication based ECC strategy is used for the got information communication. New key age strategy is presented for the expanded security level by utilizing which encryption will be performed. To stay away from the pernicious exercises verification is performed at the firewall. This confirmation is performed dependent on traffic stream. In firewall SVM calculation is carried out for the appropriate dynamic with regards to the vindictive node presence. The general examination of the exploration work is done in matlab climate from which it is demonstrated that the proposed strategies gives better and got communication over the current devices.

REFERENCE

1. Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017, May). Internet of Things (IoT) communication protocols. In *2017 8th International conference on information technology (ICIT)* (pp. 685-690). IEEE.
2. Franke, H., & Foerstl, K. (2019). Politics in internal integration for supply chain management. In *Supply Management Research* (pp. 99-108). Springer Gabler, Wiesbaden.
3. Bittencourt, L., Immich, R., Sakellariou, R., Fonseca, N., Madeira, E., Curado, M., ... & Rana, O. (2018). The internet of things, fog and cloud continuum: Integration and challenges. *Internet of Things*, *3*, 134-155.
4. Noura, M., Atiquzzaman, M., & Gaedke, M. (2019). Interoperability in internet of things: Taxonomies and open challenges. *Mobile Networks and Applications*, *24*(3), 796-809.
5. Resende, P. A. A., & Drummond, A. C. (2018). A survey of random forest based methods for intrusion detection systems. *ACM Computing Surveys (CSUR)*, *51*(3), 1-36.
6. Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247-267.
7. Kebande, V. R., Karie, N. M., Michael, A., Malapane, S. M., & Venter, H. S. (2017, May). How an IoT-enabled "smart refrigerator" can play a clandestine role in perpetuating cyber-crime. In *2017 IST-Africa Week Conference (IST-Africa)* (pp. 1-10). IEEE.
8. Moinuddin, K., Srikantha, N., Narayana, A., & KS, L. (2017). A Survey on Secure Communication Protocols for IoT Systems. *IJECS*, *6*, 21802-21807.
9. Jufri, M. T., Hendayun, M., & Suharto, T. (2017, November). Risk-assessment based academic information System security policy using octave Allegro and ISO 27002. In *2017 Second International Conference on Informatics and Computing (ICIC)* (pp. 1-6). IEEE.
10. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of things. *IEEE Communications Surveys & Tutorials*, *21*(2), 1636-1675.
11. Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 636-654). IEEE.
12. Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of things journal*, *5*(4), 2483-2495.
13. Adiono, T., Marthensa, R., Muttaqin, R., Fuada, S., Harimurti, S., & Adijarto, W. (2017, November). Design of database and secure communication protocols for internet-of-things-based smart home system. In *TENCON 2017-2017 IEEE Region 10 Conference* (pp. 1273-1278). IEEE.
14. Li, B. (2019). *Detection of false data injection attacks in smart grid cyber-physical systems* (Doctoral dissertation).

15. Porkodi, R., & Bhuvaneswari, V. (2014, March). The internet of things (IOT) applications and communication enabling technology standards: An overview. In *2014 International conference on intelligent computing applications* (pp. 324-329). IEEE.
16. Fuller, J. D., Ramsey, B. W., Pecarina, J., & Rice, M. (2016). Wireless intrusion detection of covert channel attacks in ITU-T G. 9959-based networks. In *Proceedings of the 11th International Conference on Cyber Warfare and Security* (pp. 137-145).
17. Hao, F. (2017, September). J-pake: Password-authenticated key exchange by juggling. In *International Workshop on Security Protocols* (pp. 159-171).
18. Raza, S., Duquennoy, S., Höglund, J., Roedig, U., & Voigt, T. (2014). Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN. *Security and Communication Networks*, *7*(12), 2654-2668.
19. Nir, Y., Point, C., & Kivinen, T. (2017). Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH).
20. Raza, S. (2013). *Lightweight security solutions for the internet of things* (Doctoral dissertation, Mälardalen University, Västerås, Sweden).
21. Raza, S., Shafagh, H., Hewage, K., Hummen, R., & Voigt, T. (2013). Lithe: Lightweight secure CoAP for the internet of things. *IEEE Sensors Journal*, *13*(10), 3711-3720.
22. Fernandes, J. L., Lopes, I. C., Rodrigues, J. J., & Ullah, S. (2013, July). Performance evaluation of RESTful web services and AMQP protocol. In *2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 810-815). IEEE.