International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S2, August 2019

# Keying Methods of using Protocols for Cryptography in Wireless Networks

**C. Geetha, S. Kavitha, S. Amudha**

***Abstract*: *Faraway sensor kind out breeze up obviously practical reaction for the testing troubles in different tiers, as an instance, ordinary checking, enterprise and navy packages. at ease structure customs should be obliged remote sensor systems, wherein as it has a few detainment in asset use. Sensor focus focuses are battery controlled, growing the self-enough life of a wireless Sensor Networks in a trying out improvement trouble. anyway meanwhile the rate for gobbling up noteworthiness for sensor is excessive. to vanquish this difficulty, encryption and keying strategy is applied, so that it will lessen the wide variety for transmissions used to plan the brand new key when antique key is hacked. Identified records are encoded making use of RC4 encryption estimation in this correspondence structure. in this paper we middle round encryption and keying systems that is a promising other preference to lower the structure exertion. The rekeying convention understands customer express statistics, as an example, region records as a key seed. This gadget consists of operational modes. In first gadget, each inside monitors its one – bob associates downstream focus focuses. So we reveal the entire technique to streamline the transmission of correspondence shape amidst key time through blended and keying framework.***

***Keywords – Security, WSN Security, Secure Energy Based Keying, asset obliged gadgets.***

## I. INTRODUCTION

From a protection point of view, it is fundamental to provide unfathomable shaped and right information to becoming a member of facilities and to the sink. shows ought to be with a actual goal that they're flexible in opposition to fake records pervaded into the structure by using trading topsy-turvey attention pastimes. Else the outcomes of spreading a phony statistics in a framework grow to be being stupid, debilitating the shape resources and abusing responses [1-3]. This development into a checking out to the custom creator in checking the shape. here we base on 2 keying structures. Static and Dynamic keying. In static method keys are overseeing genuinely. for example the structure center may have settled no of keys stacked. anyways, dynamic after key actual inconsistency. As such restored key would not become being any stale key. here we pivot around retaining the overhead associated with fortifying keys for the reason that correspondence price is the maximum overpowering variable. this technique performs keying limit either convulsively or on citing required via the framework. The gigantic burden of this keying tool is that it stretches out the correspondence overhead due to keys being upheld in a framework. Key refreshment can also require for assisting key. in this enterprise we develop a practical and secure correspondence structure for genius [4-8].

**Manuscript published on 30 August 2019.**
***** Correspondence Author (s)
**C.Geetha**, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India
**S.Kavitha**, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India.
**S. Amudha**, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India.



## II. BACKGROUND AND MOTIVATION

These days, the remote pioneer frameworks are nevermore early improvement and destiny advances in development can carry additionalsensor packages into our all round asked lives and in addition into modified one among a kind and testing utility things. the elementalobjective of this paper is to expose standard benchmarks to assist within the set up of relaxed WSN suggests up. recommendations for show makers to consider before an enterprise to bring together the ensured WSN shows were starting gave in [eight]. throughout this paper, we can while all is said in carried out take into account the proficient portions of safety courting from the WSNs perspective [9-12].

### A. Confidentiality

Game-plan implies the security of the recorded substance a number of the sinks and on this way the sensors. An enemy having the little bit of leeway to inclination to the substance that have to now not be able to decipher the recorded messages within the structure.

### B. Authentication

In far flung tool arranges this part tests paying little thoughts to whether or not the recorded records is transmitting from the actual blue individual from WSN. this is reliably required in light-weight of the very truth that a vindictive substance might also require the capabilityto inject imagine substance or resend a like substance into the framework. a astounding structure to conveyvalidation is use massage Authentication codes (MACs).

### C. Integrity

The recipients within the WSN must be obliged to have the option to see if the recorded substance among the exchange people from the WSN are changed, It should be constrained to make sure that the recorded substance isn't deleted, replication of past statistics, imagine or stale. Uprightness id gave through created with the aid of hashing figuring.

### D. Access Control

With discover the hazard to coordinate, unapproved usage of associate in Nursing nice is kept away from in WSNs. It watches out for that character from the shape accomplishes which substance or association. the muse riding this paper is to make up an entered and cozy correspondence structure for

WSN applications. protection (Encryption and keying) the usage of digital electricity of the machine center factor gives a method some to see statistics in line and drop fake bundles from unsafe center facilities, a brief time allotment later maintainingthe lively of the system arrange. This method firmly reinforces keys while no longer mercantilism messages for key revamping endeavors and upgrades uprightness into social events in place of structure up the organization through including MACs. The commitments to the existing paper are [13-16].

A dynamic at the methodologies separating shape that does not trade unequivocal association messages for rekeying;

Provision of 1 time keys for every wrap transmitted to preserve up a key tolerable methods from stale keys;

Well-known and all-mains protection running with a clear Device for making sure validity, persistence, and non-denial of statistics without making packs with MACs;

A shocking comfy correspondence shape this is operational in surged correspondence conditions and over precarious MACs. each descriptive and improvement comes approximately undergo witness to the chance.

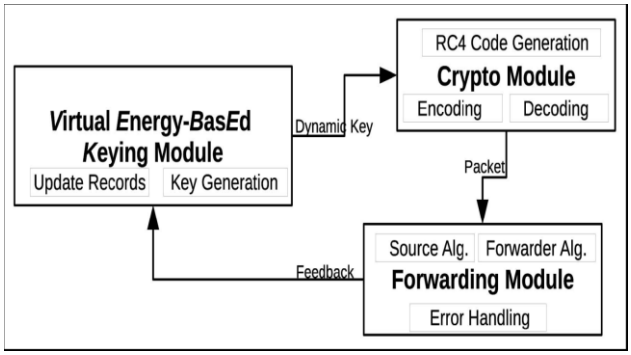


Fig 1. Modular Structure of Secure Energy based framework.possible.

**Table 1 – Notations Used**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $E_{tx}$ | Tx energy | $E_{sens}$ | Sensing energy | $E_{Fw}$ | Forwarding energy | $P_{drop}$ | Drop probability |
| $E_{rx}$ | Rx energy | $E_{sa}$ | Staying alive energy | $E_{Kdisc}$ | Key discovery energy | $\varphi$ | Synch ratio |
| $E_{comp}$ | Computation energy | $E_{vc}$ | Virtual cost | $E_{Dyn}$ | Dynamic keying cost | $l$ | packet size |
| $E_{enc}$ | Encoding energy | $E_p$ | Perceived energy | $E_{So}$ | Source node energy | $N$ | # of nodes |
| $E_{dec}$ | Decoding energy | $E_b$ | Bridge energy | $E[\eta_h]$ | Expected # of hops | $r$ | # of watched nodes |

## III. SEMANTICS OF SEBPEK

The SEBPEK structure contained 3 modules: at ease Module, Crypto Module and Forwarding.[17]

The ensured keying system blends the route of motion of dynamic keys, as other dynamic keying plans, it doesn't trade greater messages to make keys. A sensor center figures enters in placing of its brilliant centrality of the sensor. The secret is then proceeded into the Crypto module.

The Crypto module in SEBPEK makes use of a fundamental encoding method that's generally the association of time of the bits in the percent as showed up by way of the tirelessly taken off motion code made by using strategies for RC4. The sending module handles the path in the direction of sending and suffering of encoded groups while in motion to the sink.

### A. Secure Energy based Keying Module

The ensured essentialness primarily based keying module of the SEBPEK shape is one of the key obligations of this paper. It is basically the structure used for dealing with the scratching framework. It passes on a dynamic key this is then reinforced into the crypto module.

In SEBPEK each sensor center point has a particular noteworthiness regard while it's miles sent inside the shape. the assistance for using this centrality in place of actual battery ranges is that during all honesty battery tiers may additionally struggle and the restrict in the battery tiers transversely finished center facilities can also urge synchronization problems which can motive disperse.

After association, sensor middle facilities pass multiple calm wondered states. The states on a really fundamental degree be a part of middle stay-alive, % gathering, transmission, encoding, and deciphering. As those movement occur, the imperativeness in a sensor center factor is depleted. the present estimation of the centrality, Evc in internal point is used as the maximum perfect approach to manipulate supervise key time work F.

The going with check demonstrates the estimation of Dynamic key [18]

The module performs fundamental encoding venture using the period of bits within the %, as confirmed up through the proficiently taken off motion code through techniques for the RC5 encryption disconnect.

The most ideal method to manage direct RC5 is made by using digital centrality based keying module. The purpose behind the crypto module is to give clear riddle of the % header and payload whilst making sure the realness and uprightness of saw information without causing transmission overhead of widespread structures [19-21]. The gatherings combines the identity (I-bits), type (t-bits) (awaiting each center has a sort identifier), and statistics (d-bits) fields. every middle factor sends those to its next pass. RC5 encryption figuring takes the important thing and the percent fields (byte-by using-byte) as wellsprings of information and produces the end result as a segment code. the relationship of every 8-bit yield modifications into the consequent trade code. In that limit, instead of the same old technique of sending the hash regard (e.g., message systems and message endorsement codes) close to the statistics to be despatched, we use the surrendered not on time outcome of the exchange code regard regionally. To ensure rightness, the recipient isolates the plaintext identification and the decoded identification. The upsides of this concise encoding methodology are:

1) considering that there's no hash code or message framework to transmit, the get-together test does no longer make, keeping up a key now not too awful ways from bandwidthoverhead on a begin at now useful resource obliged make, on this way stirring up the shape lifetime.

2) The structure is fundamental and perfect for units with kept assets

3) The guarantee to the RC5 encryption part, to be explicit, the important thing, modifications reasonably without sending control Messages to rekey. Calculation 1.

Figure 1: Dynamic Key

```
1: ComputeDynamicKey(Evc.IDclr)
2:begin
3:j←txIDclrcnt
4: if j = 1 then
5: Kj ← F(Eini , IV)
6: else
7: Kj ← F(E(j-1) , Evc)
8: end if
9: return Kj
10: end
```

## B. Crypto module

The module performs focal encoding challenge the use of the length of bits in the %, as confirmed up by using the ably taken off motion code with the aid of strategies for the RC5 encryption discrete. The most best approach to manage direct RC5 is made by means of virtual imperativeness based keying module. the explanation behind the crypto module is to offer clear question of the party header and payload at the same time as making sure the realness and uprightness of saw facts with out causing transmission overhead of popular systems. The packs solidifies the identification (I-bits), kind (t-bits) (looking forward to each inside factor has a sort identifier), and information (d-bits) fields. every center factor sends those to its subsequent ricochet. RC5 encryption estimation takes the key and the % fields (byte-via-byte) as wellsprings of information and produces the end result as a section code. the relationship of each 8-bit yield modifications into the ensuing trade code. hence, in place of the usual manner of sending the hash regard (e.g., message structures and message announcement codes) adjacent the information to be despatched, we use the possible deferred result of the trade code regard locally. To make sure rightness, the recipient withdraws the plaintext identification and the decoded id. The upsides of this precise encoding method are:

1) since there may be no hash code or message method to transmit, the p.c. test does not make, avoiding bandwidthoverhead on a start at now resource obliged sort out, as such building up the structure lifetime.

2) The framework is important and ideal for contraptions with obliged sources three) The promise to the RC5 encryption element, to be unequivocal, the key, modifications firmly without sending manage Messages to rekey. three.3 Forwarding Module

The closing module on this correspondence plan is the sending module. it is in charge of the sending of social affairs (reports) started out at the prevailing middle point (source middle) or got packs from various sensors (sending centers) whilst in motion to the sink. The physical games of the sending module are clarified round there.

## C. Source Node Algorithm

Simply while an event is seen by a source middle, the going with stage is for the response to be asserted. The source center factor makes use of the area digital centrality regard and an IV (or beyond key regard if now not the first) to gather the going with key. For this dynamic key time strategy is generally coordinated by the SEBPEK module. The source sensor receives the present estimation of the virtual hugeness from the SEBPEK module which is used as responsibility to the RC5 figuring in the crypto module to effect a phase to code for encoding the <identification|kind|facts> message. The encoded message and the practical substance identity of the starting center are transmitted to the going with bob (sending middle or sink) the use of the going with technique: [identity; identity; kind; information laptop], in which [x]computer creates encoding x with code computer. The region virtual importance regard is reestablished and checked for use with the transmission of the going with record [22-23].

## D. Forwarder Node Algorithm

Exactly whilst the sending center factor gets the social affair it'll from the maximum punctual beginning level test its watch-once-over to pick whether or not the p.c. began from an inner factor it's far seeing. If internal factor isn't always being visible with the aid of the prevailing center, the p.c. is sent without change or sales. Overlooking the manner in which that this inner point finished rehearses on the social affair (were given and sent the p.c.), its neighboring by using virtual saw power regard is not reestablished. In case interior factor is being visible by means of the present center, the sending center point tests the related modern virtual centrality document (Algorithm2) set away for the sending center factor and focuses the imperativeness invigorating capacity to choose the important thing.

It by means of then aid the message doing away with up the message and taking flight the plaintext middle point id and the encoded center identity. If the get-together is ideal 'ol normal, a vivified virtual centrality regard is checked in the record associated with the sending middle. If the social occasion isn't always valid it's miles discarded. once more, the digital centrality regard associated with the existing sending center is starting past due vivified if this inner point has accomplished encoding on the social affair [24, 25].

**Algorithm 2.** Forwarding node algorithm with communication Error Handling

```
1:Forwarder(currentNode,WatcherNode,UpstreamNode)
2: begin
3:i← currentNode;enc←0;WL_i← WatchList
4:k←WatchedNode; src←0; j←0
5:E_rxi , ‹ID_ck , {msg}_k › ← ReceivePacket()
6:if ID_ck € WL_i then
7:   while(KeyFound = 0) and (j<=threshold) do
8:     E^k_pi ← FetchVirtualEnergy(I, ID_ck,enc,src)
9:     K← ComputeDynamicKey(E^k_pi, ID_ck)
10:   Pc←RC4(K,ID_ck)
11.   E_decri , Msg_in ← decode(Pc, {msg}_K)
12:   if ID_ck = Msg_in then
13:      KeyFound← true
14:   else
15:      j++
16: E^k_pi ← E^k_pi – E_txi –E_encri – E_rxi – E_decri – 2 * E_xi
17:   endif
18: end while
```

```
19: if keyFound=true then
20:  if j > 1 then
21:    reEncode ← true
22: else
23:   if E_ri > 0 then
24:     reEncode ← true
25:   else
26:     reEncode ← false
27:   endif
28: endif
29: if reEncode = true then
30:      enc ← 1
31:      E_xi ← FetchVirtualEnergy(I,
ID_ck,enc,src)
32:      K← ComputeDynamicKey(E_xi ,ID_ck)
33:      Pc←RC4(K,ID_ck)
34:      E_encri , {msg}_Pc ← encode(Pc,msg)
35:      packet ← ‹ID_ck , {msg}_Pc ›
36:      E_txi ← ForwardPacket()
37:      E_xi ← E_xi – E_txi –E_encri – E_rxi – E_decri – 2 *
E_xi
38:   else
39:     ForwardPacket() // Without any
modification
40:   endif
41: else
42:    DropPacket() // Packet not valid
43: endif
44: else
45: ForwardPacket() // Without any modification
46: endif
```

## IV. Operational Modes

This tradition gives three security affiliations Authentication, constancy, and non-renouncing. The focal concept behind giving those affiliations is the looking instrument. The watching framework imagines that inside facilities will store no shy of what one records(i.e., contemporary virtual criticalness level, digital stage noteworthiness regards, and Node-identification) to have the decision to figure the dynamic keys used by the supply sensor middle facilities, to loosen up social affairs and to get misled bundles either in mild of correspondence troubles or capacity ambushes. Regardless, there are expenses (correspondence, estimation, and purpose in the back of imprisonment) related with giving those affiliations.

Stage I:

within the leader mastermind operational mode, all facilities watch their friends; at something factor a social event is gotten from a neighbor sensor center, it is decoded the use of the and its dependability and uprightness are stated. essentially extremely good 'ol framed packs are despatched toward the sink. in this mode, there exists a short window of time, because it extras time for an attacker to get an inner point or get keys. After the p.c. is decoded enough, the plaintext identification is withdrawn and the decoded identification. in this framework, if the sending center factor isn't always set up to evacuate the important thing exquisitely, it will decrement the predefined virtual imperativeness regard from the present noticed centrality (line sixteen in algorithm 2) and attempts any other key before portraying the p.c. as ruinous. If the social event is tremendous 'ol formed, and this influence isn't the closing ricochet, the p.c. is re-encoded by way of the sending center factor with its very personal stand-out specific key got from its contemporary digital level importance stage. In case the social event is insane, the p.c. is discarded. This shape continues till the factor that the instant that the social occasion accomplishes the sink. In like way, unusual movement is remoted earlier than it enters the shape. Re-encoding at each ricochet vivifies the possibility of the encoding. The degree decreases the transmission overhead because it will absolute confidence get noxious applications in the going with pass, at any fee creates managing overhead in mild of the resolve.

Stage II:

Within the stage II operational mode, center obsessions inside the framework are proposed to without a doubt watch a dash of internal concentrations inside the shape. each internal point heedlessly choices r facilities to display screen and stores the touching on state earlier than alliance. As a percent leaves the source center (beginning center factor or sending center factor) it reports node(s) that watch it probabilistically. In case the existing center point is not seeing the center that made the social affair, the % is sent. In case the middle that made the social event is being seen by way of the existing middle factor, the p.c. is decoded and the plaintext identification is limited and the decoded id. Like level I, if the watcher-forwarder middle factor can not find the important thing tastefully, it'll strive a questionable quantity of keys

from the estimation of digital KeySearch Threshold earlier than truly referencing the party as undermining. If the get-collectively is fundamental, and this pass isn't always the last objective, the administrator proper despatched aside from if the center is starting at now go the framework. within the crossing factor case, the critical % is re-encoded with the virtual improvement vitality and despatched. This operational mode has more transmission overhead for the reason that packs from a unsafe center factor might be gotten by means of a watcher center and they will accomplish the sink. anyhow, instead of the stage I mode, it reduces the supervising overhead (in mild of the manner that much less re-encoding is done and unwinding up isn't always done at every ricochet). The change off is that a silly assembling might also examine some skirts early being dropped [26-30].

## V. PERFORMANCE ANALYSIS

Here we survey the feasibility of the SEBPEK framework by methods for the two multiplications and examination.

### A. Assumptions

In mild of the bypass on thought of the far off medium used as a dash of sensor structures, aggressors may undertaking to concentrate stealthily, get, or drench false messages. in this paper, we overwhelmingly bear in mind the fake blend and listening stealthily of messages from an outside perilous middle; along these traces, as [12], insider ambushes are out of doors the degree of this paper. This aggressor is thought to have an appropriate repeat, custom, and perhaps a reprimanded liberal center point identification. all through this work, the going with suppositions are apart from made:

- Directed Diffusion [7] controlling custom is used, but others, as an instance, [8] can in like way be used. As showed up via primary functions of Directed Diffusion, after the sink demands statistics via interest messages, a controlling manner is created making use of the assets inside the occasion territory to the sink. We see that the manner is settled within the midst of the progress of the facts and the route method is secure.
- The arranging estimation is sent on a plotting medium get right of entry to control display up. The shape may enjoy ACK or facts assign.
- The sensor structure can also thickly populated with an authoritative goal that specific sensors watch and make reports for identical event.
- Sensors are believed to have a basically ambiguous correspondence runs and can have specific rapidly battery suppliers.

### B. Simulation parameters

We use the Georgia Tech Sensor network Simulator(GTSNetS)[three], which is an event primarily based talk shaped sensor virtuoso take a look at framework with C++, as our preoccupation degree to play out the evaluation of the SEBPEK correspondence structure, the topology used for the starting is confirmed up in fig.2., at the same time as the parameters used as a touch of the reenactment are delineated out in table 2 and three. cognizance focuses were dispersed abstractly within the sending zone and all around, the p.c. between the supply focus fixations and the sink become around 25-35 trusts.Fig 2. Simulation Topology with GTSNetS.

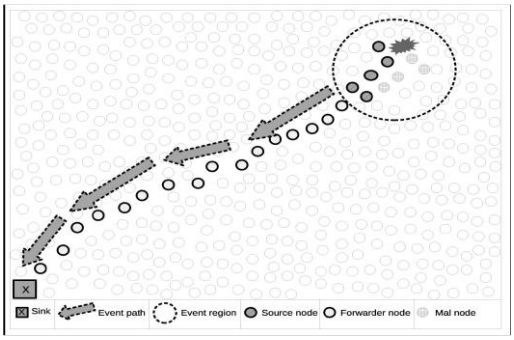


Table 2. Energy related Parameters

| | | | |
|---|---|---|---|
| $E_{rx}$ | 85.1$\mu$J | $E_{dec}$ | 15.5$\mu$J |
| $E_{tx}$ | 78$\mu$J | $E_{enc}$ | 15.5$\mu$J |
| $E_{sens}$ | 36$\mu$J | Voltage | 3V |
| $E_{sa}$ | 18.6$\mu$J | | |

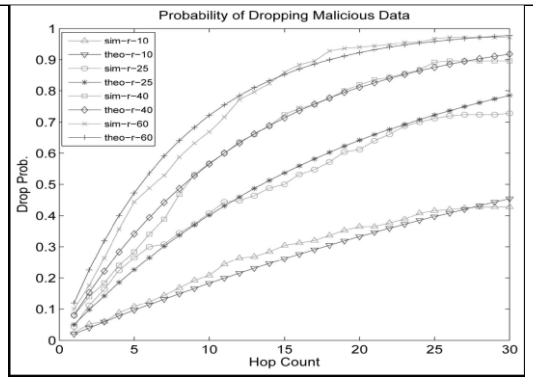


Fig.3 Theoretical and simulation results with varying number of watched nodes.

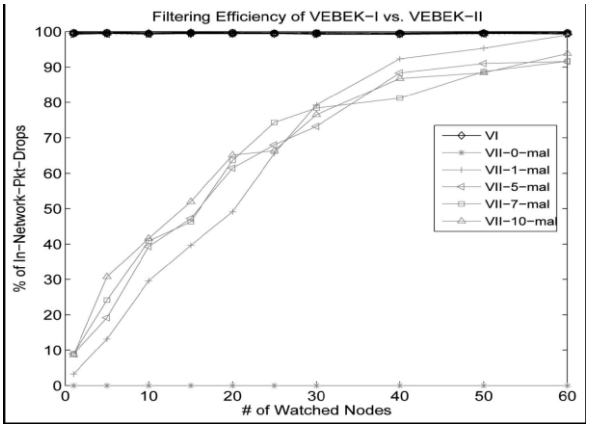


Fig 4. Comparison of filtering efficiency for SEBPEK-Phase II with varying number of malicious nodes.

## VI. CONCLUSION

In evaluation with other key affiliation systems, SEBPEK has the going with vital focuses: 1) it does not trade manage messages for input duplicating endeavors and is for this reason treated to store gradually fundamental centrality and is much less plenteous, 2) it uses one key for every message so thoughts blowing gatherings of the circulation use gathered keys—making SEBPEK greater grounded to specific attacks (e.g., replay ambushes, creature oblige strikes, and unfold ambushes), and 3) it unbundles

key period from protection affiliations, giving a versatile isolated structure that considers a rapid storing of various key-based encryption or hashing plans.

We've surveyed SEBPEK's plausibility and execution thru each hypothetical evaluation and reenactments. Our outcomes exhibit that specific operational systems for SEBPEK (segment-I and section-II) can be made to offer perfect execution in a social occasion of structure plans depending, in a way, on using the sensor engineer. We in like manner taken into consideration the centrality execution of our structure with other being evolved dangerous facts limiting plans.

## REFERENCES


1. Gowri Sankaran, B., Karthik, B. & Vijayaragavan, S.P. 2019, "Weight ward change region plummeting change for square based image huffman coding", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 4313-4316.
2. Gowri Sankaran, B., Karthik, B. & Vijayaragavan, S.P. 2019, "Image compression utilizing wavelet transform", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 4305-4308.
3. Kandavel, N. & Kumaravel, A. 2019, "Offloading computation for efficient energy in mobile cloud computing", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 4317-4320.
4. Vinoth, V.V. & Kanniga, E. 2019, "Reversible data hiding in encrypting images-an system", International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 3051-3053.
5. Selvapriya, B. & Raghu, B. 2019, "Pseudocoloring of medical images: A research", International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 3712-3716.
6. Senthil Kumar, K. & Muthukumaravel, A. 2019, "Bi-objective constraint and hybrid optimizer for the test case prioritization", International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 3436-3448.
7. Kavitha, G., Priya, N., Anuradha, C. & Pothumani, S. 2019, "Read-write, peer-to-peer algorithms for the location-identity split", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 445-447.
8. Kaliyamurthie, K.P., Michael, G., Anuratha, C. & Sundaraj, B. 2019, "Certain improvements in alzheimer disease classification using novel fuzzy c means clustering for image segmentation", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 599-604.
9. Kaliyamurthie, K.P., Sundarraj, B., Geo, A.V.A. & Michael, G. 2019, "RIB: Analysis of I/O automata", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1019-1022.
10. Velvizhi, R., Rajabhushanam, C. & Vidhya, S.R.S. 2019, "Opinion mining for travel route recommendation using Social Media Networks (Twitter)", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 508-512.
11. Kavitha, R., Sangeetha, S. & Varghese, A.G. 2019, "Human activity patterns in big data for healthcare applications", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1101-1103.
12. Pothumani, S., Anandam, A.K., Sharma, N. & Franklin, S. 2019, "Extended VEOT framework - Implemented in a smart boutique", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 762-767.
13. Kaliyamurthie, K.P., Michael, G., Krishnan, R.M.V. & Sundarraj, B. 2019, "Pseudorandom techniques for the internet", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 915-918.
14. Aravindasamy, R., Jeffrin Rajan, M., Rama, A. & Kavitha, P. 2019, "Deep learning provisions in the matlab: Focus on CNN facility", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 990-994.
15. Theivasigamani, S., Linda, M. & Amudha, S. 2019, "Object sensing and its identification & motion sensing", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 545-549.
16. Mary Linda, I., Vimala, D. & Shanmuga Priya, K. 2019, "A methodology for the emulation of IPv4", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 848-852.
17. Velvizhi, R., Priya, D.J., Vimala, D. & Linda, I.M. 2019, "Increased routing algorithm for mobile adhoc networks", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1606-1608.
18. Sangeetha, S., Anuradha, C. & Priya, N. 2019, "DNS in real world", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 937-940.
19. Geetha, C., Vimala, D. & Priya, K.S. 2019, "Constructing multi-processors and spreadsheets with SKIVE", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 516-519.
20. Yugendhar, K., Sugumar, V. & Kavitha, P. 2019, "A novel method of univac using fuzzy logic", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 435-437.
21. Kaliyamurthie, K.P., Michael, G., Elankavi, R. & Jijo, S.A. 2019, "Implementing aggregate-key for sharing data in cloud environment using cryptographic encryption", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 957-959.
22. Jeffrin Rajan, M., Aravindasamy, R., Kavitha, P. & Rama, A. 2019, "A novel method of object orientation variation in C++ and java", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 708-710.
23. Nayak, R., Dinesh, S. & Thirunavukkarasu, S. 2019, "A novel method improvement of rapid miner for the data mining applications", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 457-460.
24. Sivaraman, K., Krishnan, R.M.V., Sundarraj, B. & Sri Gowthem, S. 2019, "Network failure detection and diagnosis by analyzing syslog and SNS data: Applying big data analysis to network operations", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 883-887.
25. Vimala, D., Linda, I.M. & Priya, K.S. 2019, "Decoupling online algorithms from erasure coding in DNS", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 950-953.
26. Rama, A., Kumaravel, A. & Nalini, C. 2019, "Preprocessing medical images for classification using deep learning techniques", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 711-716.
27. Sangeetha, S., Srividhya, S.R., Anita Davamani, K. & Amudha, S. 2019, "A procedure for avoid overrun error in universal synchronous asynchronous receiver transmitter (usart) by utilizing dummy join and interrupt latency method", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 657-660.
28. Aravindasamy, R., Jeyapriya, D., Sundarajan, B. & Sangeetha, S. 2019, "Data duplication in cloud for optimal performance and security", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1156-1158.
29. Aravindasamy, R., Jeffrin Rajan, M., Sugumar, V. & Kavitha, P. 2019, "A novel method on developing superblocks and the transistor using apodryal", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 982-985.
30. Sasikumar, C.S. & Kumaravel, A. 2019, "E-learning attributes selection through rough set theory and data mining", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 3920-3924.


## AUTHORS PROFILE

**C. Geetha** Assistant Professor, Department of Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, India

**S.Kavitha** , Assistant Professor, Department of Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, India

**S. Amudha,** Assistant Professor, Department of Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, India