PROVIDING SECURITY SOLUTION TO DATA FROM IOT DEVICES USING HIGH SCALABLE LIGHT WEIGHT SECURITY ALGORITHMS OVER WIRELESS NETWORKS

SATISHA C[1], Dr RAGHAV MEHRA[2]

[1] Research Scholar, Department of Computer Science, Bhagwant University, Ajmer,
csscholar96@hotmail.com
[2] Associate Professor & Assistant Director, BIT-Bhagwant Institute of Technology, Muzaffarnagar,
raghav.mehrain@gmail.com

ABSTRACT

Now a day's Internet of Things (IOT) is plays vital role in communication technologies. IOT devices can be extracted data and same data can be used in many inter disciplinary applications. Providing security to IOT data is also big challenging task. Enormous number of algorithms is developed by researchers to provide security to network data but a light weight security model is preferred for IOT data. In this research paper we are working on IoT channel attack where IoT devices are deployed without security mechanisms or semi security algorithms. We conducted cryptanalysis on Advanced Encryption Standard (AES) algorithm which is available on open source, it is possible to force channel attack, and attacker has no control on input data. In this research we proposed a new scalable secure technique to protect channel data from IoT channel attack. We analyzed non linearity of s boxes used by various single key crypto algorithms by changing selection function. Various metrics like transparency order, guessing entropy, success rate, and correlation coefficient are used to study various cryptography algorithms.

Keyword: - *IOT channel attacks, IOT network security models, Security of S-boxes, selection functions, DPA and CPA attacks, Attacker*

1. INTRODUCTION

Metropolitan urban communities all around the world are utilizing IOT gadgets, It's been IoT to IoE (Internet of Everything) time, Sapless security could impact the presences of millions of clients assurance, Security and Trust. 2021 has similarly been the hour of overall computerized settlements to help with obstructing attacks [8]. Security perils are any place the ordinary Insider risks or Zero-day attack continues to go a typical of eight months or years without knowing it. That delivery attacks adequate chance to take significant assets. Due to number moreover kinds of shortcomings continuing to grow drastically with the spread of ascent of IoT, Anti-infection and understanding deals with make such a ton of data advancements to assemble, analyze, besides report data network configuration is only a huge part of the battle, completes controls [19]. The present IoT related risks need a point by point event response procedure when it has an effect on follow when you become entered [8].

The central highlight of their investigation is to include huge security issues of IoT particularly, focusing the security attacks and their countermeasures. Due to nonattendance of wellbeing instrument in IoT contraptions, various IoT devices become simple targets and without a doubt, even this isn't in the loss' data on being spoiled [2]. The security necessities are inspected like protection, uprightness, and approval, etc In their composing study, twelve unmistakable sorts of attacks are requested as low-level attacks, medium-level attacks, evident level attacks, and exceptionally critical level attacks close by their tendency/direct as well as proposed deals with serious consequences regarding experience these attacks are discussed [10]. Considering the meaning of wellbeing in IoT applications, it is really fundamental to present security framework in IoT devices and correspondence associations. Moreover, to safeguard from any intruders or security risk, it is similarly endorsed not to include default passwords for the contraptions and read the security requirements for the devices proceeding including it curiously. Crippling the features that are not used may lessen the potential outcomes of security attacks. Also, it is fundamental for focus on different security shows used in IoT devices and associations [14].

Finally, the different attack vectors of the IoT are upsetting. Despite the current Internet risks, there are different new vectors presented [3]. The open and public nature of various IoT structures makes them especially vulnerable against malicious attacks. This is moreover underlined by the routinely powerless security sent into the genuine contraptions. Correspondence by radio waves is frail to numerous sorts of attacks, going from tuning in to without a doubt DoS attacks [18]. The lacking prerequisite methodologies makes this fundamentally more limit, making extra strain for the systems to be as screw up permissive as could truly be anticipated. Accepting security continues to be an outrageous issue in IoT, it could at last hinder development gathering by end clients and thusly deferred down the field's new development. Further, investigation and review attempts are expected in aiding device makes, regulators, and implementers to zero in on tries while making IoT security frameworks [12].

2. RELATED WORK

The Internet of Things (IoT) thought is emerging and growing rapidly. Different particular solutions for a seriously prolonged stretch of time have been proposed for its execution. The quick headway and use of IoT progressions has raised security concerns and made a vibe of weakness among IoT adopters [17]. Makers examine the back and forth movement research designs associated with security stresses of the IoT thought and give an unmistakable perception of the subject. They applied exact arranging study as the foundational system [15]. Considering the picked search method, they picked research papers for a closer appraisal. Out of these articles, the concerns, courses of action and investigation openings for the security in the IoT thought were isolated. The arranging focus on perceives nine essential concerns and 11 courses of action. Regardless, the disclosures moreover uncover troubles, for instance, secure insurance the board cloud blend that really requires useful courses of action [16]. Their assessment work has shown how the security stresses in the IoT space have created. The deliberate arranging communication of this study reveals how the headway has happened, what kinds of stresses and game plans exist, and what openings remain [20].

The current revelations show that IoT security very gigantic work before it is ready for all over open affirmation. Various security concerns endure. The most inescapable are security concerns, ID, approval and approval concerns and nonappearance of the leaders systems. Security in the IoT is basic, as the contraptions used regularly accumulate private, individual data, such as prosperity information [11]. Much has been done to get sensitive clients' data, similar to individual information and real characteristics, through check procedures, for instance, data based affirmation, and clients' own understanding based approval with splendid cards or access cards, and real credits. Regardless, they don't change to the heterogeneous and resource obliged environment of the IoT [3]. Similarly, amazing work has been done to either change the current shows for IoT purposes or foster absolutely new ones for lightweight encryption and secure association transmission [5]. Considering this current audit's outcomes, the most lacking with respect to part of the IoT security is correct now affirmation and approval. Then, at that point, growing number of IoT contraptions in clients' ordinary schedules make confirmation and security fundamental. After approval, the entry control issue ought to be tended to, as few out of every odd individual gets to everything. Various researchers present this as a significant inquiry to address, but these revelations suggest an inescapable, capable and adaptable response for IoT approval issues is missing [7].

All through the whole presence of contraption enlisting, Internet of Things (IoT) is one of the fastest creating field that going up against various security challenges. The effective undertakings should have been made to address the security and assurance issues in IoT associations. The IoT contraptions are on a very basic level resource control device which gives routine attracts impression to computerized aggressors. The IoT collaboration centers are extending rapidly with more resource constrained that making extra troublesome conditions in the persistent. The current procedures give an ineffective response to the tasks for convincing IoT device. Furthermore, it is a lacking to incorporate the complete security and prosperity scope of the IoT associations [1]. Because of the current computations are not progressed to get IoT bionetwork in the persistent environment. The current structure isn't with the eventual result of recognizing the mediator to the endorsed person in the embedding devices. Similarly, those methods are had confidence in single model region. As such, the suitability is dropping for extra multimodal space like blend of social and physiological components. The introducing sharp strategy will be securitizing for the IoT devices and associations by profound learning (DL) methodologies. The DL procedure is keeping an eye on different security and prosperity issues arise continuously environment. in their investigation they are including cream DL techniques with Reinforcement Learning (RL) for the better show during attack and differentiated and existing one. Moreover, here they inspected concerning DL got together with RL of a couple of procedures and perceive the higher accuracy estimation for security plans [1].

Remote correspondence networks are uncommonly disposed to security risks. The huge uses of distant correspondence networks are in military, business, clinical benefits, retail, and transportations. These systems use wired, cell, or ad-hoc networks. Distant sensor associations, actuator associations, and vehicular associations have gotten a phenomenal thought in the public eye moreover industry [6]. Recently, the IoT has gotten huge assessment thought. The IoT is considered as possible destiny of the web. In future, IoT will expect a basic part and will change our living styles, standards, as well as game plans. The use of IoT in different applications is depended upon to rise rapidly after a short time. The IoT licenses billions of devices, social classes, and organizations to connect with others and exchange information. In view of the extended utilization of IoT contraptions, the IoT networks are leaned to various security attacks. The sending of capable security and insurance shows in IoT networks is unquestionably expected to ensure mystery, approval, access control, and uprightness, among others. In their assessment they gave a wide extensive review on security and assurance issues in IoT networks is given [13].

IoT is an organization of material article associated through web. Material articles embedded with RFID, WSNs and much more through which things stay related with each other. Each material article which is the piece of correspondence are having an intriguing identifier. IoT is extremely heterogeneous, so security is a significant test in IoT. In their investigation various security challenge and counters measures and assessment objections are considered [4]. The principal commitment of this work is to contemplate the support of IoT by various assessments; and after that security challenges in IoT subject to different audits the vision and security issues; bets on Perception Layer; and various applications. The inspiration driving this outline has been made by giving a good review of the assessment floats in IoT security. To abbreviate, the IoT is a sort of arrangement of a couple of real gadgets or things which, embedded with programming, sensors and structure that enables them, achieves continuously noticeable worth and relationship by exchanging data with creators, managers and a couple of other related contraptions. Thusly, the concentrated evaluations and the mass taking care of, which are stayed aware of by mists, are as habitually as possible inefficient. A couple of models harden the impediments of limit, correspondence limits, dealing with and power. Future headings of this blueprint solidify working up on a safe and hazard free IoT model, trailed by getting sorted out a zero trust calculation to ease known and cloud progressed assaults on an IoT system [4].

3. IOT CRYPTOGRAPHY SECURITY MODEL

IOT channel attacks forced by attacker to hake sensitive useful data from channel IOT devices or end to end users. Channel attack is a one of the problem occurred due to non implementing security techniques to channel. These kinds of attacks encountered at runtime. At the time of design security provided using many symmetric cryptography algorithms and when attacker forcing channel attack it behaves differently based on algorithm. A simple IOT security model is shown in figure 1.

Notations used:

M^+ → Modular addition

M^- → Modular subtraction

M_B → Most significant byte of y

L_B → Least significant byte of y

S_{bc} → S Box of block cipher

H_D → Hamming Distance

H_W → Hamming Weight

H_D (a, b) → Hamming distance of a & b

H_W (a) → Hamming weight of a

P_C → Product Cipher

Nr → Number of rounds

$C^{(0)}$ → Plain text

C^{Nr} → Cipher text

n → block size in bits

R_F → Round function

+ → Addition over Z

$\oplus$ → Addition mod2 over Z

P → Plain Text

C → Cipher text

NL → Non linearity

T_O → Transparency Order

S_R → Success Rate

E_G → Guessing Entropy

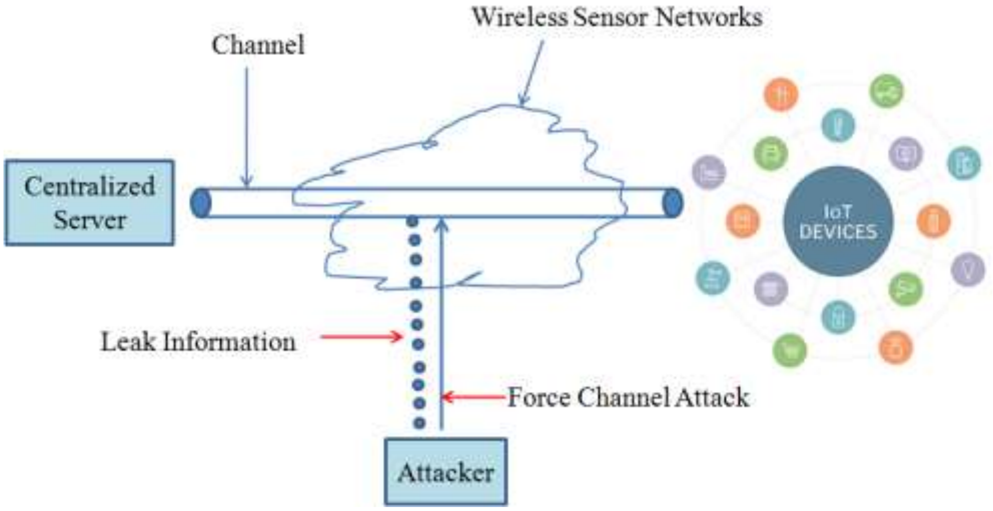

Fig -1: IOT Security network model

A product cipher text can be calculated by running round function into N_r times. Cipher product is calculated by using following equation.

$$C^{(Z)} = R_K (C^{(Z-1)}) \text{ for all } N_r \geq Z \geq 1$$

Selection function f will give better results in case of IOT devices. Attacker immediately force channel attack to extract secret key by using a small value called $\propto$. $\propto_r = \propto (c, r)$, where c is a part of C^{Z-1} of R_F. r is a unknown portion of R_k. Attacker may did cryptanalysis to know value of $\propto_r$ (immediate) for known c value and for all combination of keys r. bitwise of |r| of key r may used to calculate memory size required to force IoT Channel attack. Attacker may use values $\propto_1$, $\propto_2$, $\propto_3$, ………, $\propto_r$ and IOT channel leak to know exact round key during data transfer between IOT devices. Attacker may use more number of c to leak channel data which in turn useful to extract r. function f is selected to complete each round of encoding or decoding operation. Let a pair of vectors g = (g_1, g_2, …..,g_t) and h = (h_1, h_2, …., h_t). S boxes are a one of the simplest way to maintain N_L in single key cryptography algorithms. S box is a (k, t) function f, $f: f_2^k \rightarrow f_2^t$, f is used to map k input to t output bits. F is a simply a Boolean function if t=1 or otherwise f (y) = (f_1(y), f_2(y), ….., f_t (y))

Walsh transform W_T (i, j) = $\sum_{x\in f_2^k}(-1)^{if(y)+jx}$

N_L of (k, t) is a function f can be defined as

$$N_L\,(f) = 2^{k-1} - \frac{1}{2} max_{j\in f_2^t,\ i\in f_2^k} |W_T\,(i,j)|$$

T_O of (k, t) of f is defined as

$$T_O = (max_{\propto\in f_2^t}(|t - 2\,H_W\,(\propto)|) - \frac{1}{2^{2^k} - 2^k}\sum_{i\in f_2^k}\sum_{j\in f_2^t}|(-1)^{j.\propto}\,W_T(0,j)\,|)$$

T_O (f) Value lies between 0 to t. k and t are two integers. Transparency order function is useful to protect S box from differential power analysis attacks. High value of T_O(f) protect more from differential power analysis attacks.

4. RESULTS AND DISCUSSIONS

Selection function $\propto (c,r)$ used to guess round keys. Attacker may guess different sub keys for different rounds. g_kGuess key vector. $g_k$can be defined as $g_k = \{ g_1, g_2, g_3, \ldots\ldots, g_k\}$. Two metrics are used to extract exact sub key from g_k. They are success rate and Guessing entropy. Attacker may force attacks many times using different queries and S_R of these queries to identify exact sub key is defined as

$$S_R(R_k, g_k) = \begin{cases} 1 & if\ R_k \in \{g_1, g_2, g_3, \ldots\ldots, g_k\} \\ 0 & Otherwise \end{cases}$$

Entropy of identifying exact or appropriate key using channel attack can be defined as

$$E_G\,(R_k, g_k) = log_2^{g_k} for\ all\ g_i \in \{g_1, g_2, g_3, \ldots\ldots, g_k\}$$

Algorithm to evaluate correlation power analysis CPA attacks

Step 1: for i=1 to N_E do

```
Step 2: Power traces ($R_k$, query)
Step 3: for j=1 to q do
Step 4: $g_k = CPA\ (C, j, t)$
Step 5: Calculate $S_R^{i,j}(R_k, g_k)$, $E_G(R_k, g_k)$
Step 6: end for
Step 7: for k = 5 to query do
Step 8: calculate $S_R = \frac{1}{N_t} \sum_{i=1}^{N} S_R^{i,k}(R_k, g_k)$
Step 9: calculate $E_G = \frac{1}{N_t} \sum_{j=1}^{N_E} E_G^{i,k}(R_k, g_k)$
Step 10: end for
Step 11: end for
```

Data leakage is also one of the problems where attacker may execute instructions which in turn consume power of IOT devices. To understand IOT device data leakage we evaluated five instructions which are using registers and memory. Instructions operate on registers, first one is add instruction a + b, and second one is and instruction a ∧ b. Instructions operate on memory, lpm instruction is used to read data from flash memory to registers, load instruction read data, and store instruction write data to register. AES Security algorithm uses S box with an index to perform ⊕ operation over plaintext and key to access memory location. Experimental results have shown in table 1 shows how instructions leak data about keys. Correction coefficient is defined as a difference between correlation of exact key and correlation of approximately close to key. From our experiments we come to know that attacker may force attacks to increase success rate with help of α value.

Table -1 Correlation coefficient (instructions Vs Correct secret sub key)

Instructions/ Correct Sub key	∧	+	Load	store	LPM
0X00	-0.789	0.210	0.255	0.599	0.382
0X01	-0.639	-0.219	0.210	0.584	0.322
0X03	-0.568	-0.170	0.184	0.581	0.299
0X05	-0.545	-0.111	0.191	0.577	0.244
0X07	-0.520	-0.081	0.231	0.571	0.221
0X0F	-0.456	-0.055	0.214	0.567	0.185
0X1F	-0.394	0.002	0.228	0.592	0.171
0X3F	-0.334	0.051	0.212	0.602	0.166

0X5F	-0.201	0.047	0.205	0.594	0.161
0X7F	-0.182	0.042	0.196	0.587	0.157
0XFF	-0.021	0.002	0.219	0.593	0.146
β	-0.426	-0.031	0.215	0.589	0.219

From our experimental results store instruction leaks more than load instruction, other hand $\wedge$ operation leaks less than 18 times approximately when compared with + operation. We conducted experiments by changing selection functions. Let the following are list of selection functions.

$$\propto_1 (a,b) = a \wedge b$$

$$\propto_2 (a,b) = a \vee b$$

$$\propto_3 (a,b) = a \oplus b$$

$$\propto_4 (a,b) = a\ M^+\ b$$

$$\propto_5 (a,b) = S_{AES}(a \oplus b)$$

$$\propto_6 (a,b) = S_{PRINCE}(a \oplus b)$$

$$\propto_7 (a,b) = S_{RC5}(a \oplus b)$$

$$\propto_8 (a,b) = S_{LBLOCK}(a \oplus b)$$

$$\propto_9 (a,b) = S_{FANTOMAS}(a \oplus b)$$

We conducted experiments by changing various selections, where selection function writing data to memory using store instruction may leak more information compared with other instructions. In table 2 listed various selection functions, non linearity of each selection functions, and value of β. Data leakage of various selection functions $\propto_i$ are listed in table 3.

Table -2 Leakages values of various selection functions

	$\propto_1$	$\propto_2$	$\propto_3$	$\propto_4$	$\propto_5$	$\propto_6$	$\propto_7$	$\propto_8$	$\propto_9$
k (i/p)	16	16	16	16	8	8	16	4	8
t (o/p)	8	8	8	8	8	8	8	4	8
N_L	16392	16392	0	-0.149	112	64	0	4	0
β	-0.006	-0.019	0	0.131	0.571	0.141	0.247	0.351	0.139

Table -3 Detailed leakage values of selection function $\propto_i$ in table 2.

	$\propto_1$	$\propto_2$	$\propto_3$	$\propto_4$	$\propto_5$	$\propto_6$	$\propto_7$	$\propto_8$	$\propto_9$
0X00	-0.219	0.097	0.092	0.071	0.053	-0.029	-0.049	-0.002	0.009
0X01	0.007	-0.006	-0.001	-0.069	-0.001	0.031	0.019	0.081	-0.198
0X03	-0.151	-0.159	-0.169	-0.188	-0.166	0.150	-0.139	-0.127	-0.127
0X05	0.588	0.579	0.571	0.569	0.564	0.591	0.599	0.581	0.587
0X07	0.337	0.339	0.333	0.349	0.334	0.124	0.119	0.094	0.129
0X0F	0.241	0.231	0.235	0.251	0.233	0.249	0.248	0.235	0.233
0X1F	0.257	0.251	0.271	0.263	0.267	0.271	0.266	0.259	0.272
0X3F	0.101	0.091	0.081	0.068	0.069	0.079	0.109	0.101	0.125
0X5F	0.039	0.031	0.031	0.031	0.021	0.049	0.061	0.069	0.071
0X7F	0.151	0.132	0.142	0.131	0.130	0.150	0.135	0.152	0.145
0XFF	0.081	0.081	0.039	0.040	0.083	0.099	0.130	0.099	0.099

5. CONCLUSION

IOT is one of the emerging fields and these kinds of devices are used in many inter-disciplinary applications. In this research paper we conducted research on IOT network security model. We are conducted various experiments to protect IOT channel data from IOT channel attacks. In correlation power analysis (CPS) context we conducted experiments and from our study we identified data leakages done mainly due to attack on selection function. Operations like + and $\wedge$ may leak less data than what attacker expected and this not fully useful to extract exact secret key. In case of block cipher algorithm usage of 4 bit s box and 4 bit selection is shows better results that 8 bit s box and 8 bit selection function. L boxes used by fantomas may leak more data that what attacker may expected and this is one of the selection function to force CPA attack to leak secret key.

6. REFERENCES

[1]. Chen, J.I.Z., Lai, K.L., “Internet of Things (IoT) Authentication and Access Control by Hybrid Deep Learning Method - A Study”, Journal of Soft Computing Paradigm, vol. 02, no. 04, pp. 236-245, 2020.

[2]. Wan, J., Tang, S., Shu, Z., Li, D., Wang, S., Imran, M., Vasilakos, A.V., “Software-defined industrial internet of things in the context of industry”, IEEE Sensors Journal, vol. 16, no. 20, pp.7373–7380, 2016.

[3]. Porras, J., Pankalainen, J., Knutas, A., Khakurel, J., “Security In The Internet Of Things – A Systematic Mapping Study”, Proceedings of the 51st Hawaii International Conference on System Sciences, ISBN: 978-0-9981331-1-9, pp. 3750-3759, 2018.

[4]. Mukhandi, M., David, P., Pereira, S., Couceiro, M.S., “A novel solution for securing robot communications based on the MQTT protocol and ROS”, IEEE SICE International Symposium on System Integration, pp. 608–613, 2019.
[5]. Rwan, M., Yousuf, T., Aloul, F., Imran, Z., “Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures”, the 10th IEEE International Conference for Internet Technology and Secured Transactions, ISBN: 978-1-908320-52/0, pp. 336-341, 2015.
[6]. Navneet, V., Suman, S., Sukhdeep, S., Devender, P., “IoT Security Challenges and Counters Measures”, International Journal of Recent Technology and Engineering, ISSN: 2277-3878, vol. 8, no. 3, pp.1519-1528, 2019.
[7]. Mohit Kumar, S., Rakesh Kumar, S., “Internet of Things (IoT) Applications and Security Challenges: A Review”, International Journal of Engineering Research & Technology, ISSN: 2278-0181, vol. 7, no. 12, pp. 1-8, 2019.
[8]. Rutten, E., Marchand, N., Simon, D., “Feedback control as MAPE-K loop in autonomic computing”, Software engineering for self-adaptive systems III Assurances, Springer, Cham, pp 349–373, 2017.
[9]. Mavrogiorgou, A., Kiourtis, A., Perakis, K., Pitsios, S., Kyriazis, D., “IoT in healthcare: achieving interoperability of high-quality data acquired by IoT medical devices”, Sensors, vol. 19, no. 1978, pp. 1-24, 2019.
[10]. Coman, F.L., Malarski, K.M., Petersen, M.N., Ruepp, S., “Security issues in internet of things: Vulnerability analysis of LoRaWAN, sigfox and NB-IoT”, International Conference on Global IoT Summit, IEEE, pp 1–6, 2019.
[11]. Blessy, S., Priya, D., “Building Greater Iot Security And Trust”, International Journal of Research and Analytical Reviews, E-ISSN 2348-1269, P- ISSN 2349-5138, vol. 5, no. 3, pp. 62-67, 2018.
[12]. Lemayian, J.P., Turjman, F., “Intelligent IoT communication in smart environments: an overview”, Transactions on Computational Science and Computational Intelligence In: Artificial Intelligence in IoT, Springer, Cham, pp 207–221, 2019.
[13]. Sinh, D., Le, L.V., Lin, B.S.P., Tung, L.P., “SDN/NFV—a new approach of deploying network infrastructure for IoT”, International conference on Wireless and optical communication conference, IEEE, pp 1–5, 2018.
[14]. Zhang, Z.K., Yi Cho, M.C, Wang, C.W., Hsu, C.W., Chen, C.K., Shieh, S., “IoT Security: Ongoing Challenges and Research Opportunities”, 2014 IEEE 7th International Conference on Service Oriented Computing and Applications, ISBN: 978-1-4799-6833-6/14, pp. 230-234, 2014.
[15]. Safkhani, M., Bagheri, N., “Passive secret disclosure attack on an ultra light weight authentication protocol for internet of things”, Journal of Super computing, vol. 73, no.8, pp 3579–3585, 2017.
[16]. Sachin, K., Tiwari, P., Zymbler, M., “Internet of Things is a revolutionary approach for future technology enhancement: a review”, Springer Journal of Big Data, pp. 1-21, vol. 6, no. 111, 2019.
[17]. Sidorov, M., Ong, M.T., Sridharan, R.V., Nakamura, J., Ohmura, R., Khor, J.H., “Ultra light weight mutual authentication RFID protocol for block chain enabled supply chains”, IEEE Access, vol. 7, pp.7273–7285, 2019.
[18]. Ashok Kumar, N.R., Chandrakala, B.M., “IoT Security Threats and Risks Mitigation Information Security Threats by “One Alert Way”, International Journal of Engineering Research and Technology, ISSN: 2278-0181, vol. 4, no. 29, pp. 1-3, 2016.
[19]. Alam, S., Siddiqui, S.T., Ahmad, A., Ahmad, R., Shuaib, M., “Internet of Things (IoT) enabling technologies, requirements, and security challenges”, Advances in data and information sciences, Springer, Singapore, pp 119–126, 2020.
[20]. Razzaq, M.A., Qureshi, M.A., Gill, S.H., Saleem, U., “Security Issues in the Internet of Things (IoT): A Comprehensive Study”, International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, pp. 383-388, 2017.

	Satisha C Satisha C is from Bangalore, Karnataka and pursuing PhD from Bhagwant university on the topic " A new secure algorithm to protect data leakage from IOT devices over wireless Network". He has completed bachelor's degree BSc in computer Science and Masters degree MCA from Bangalore University. Currently he is working as Asst. Professor, Department of Computer Science, Sree Siddaganga College of Arts, Science and Commerce, Tumkur. The author attended many National and international conferences. Recently published research paper / article ' A survey on overview of Security protocols, Mechanisms, Attacks, Applications suitable for IOT devices over wireless Networks".
	Dr. Raghav Mehra Dr. Raghav Mehra is Associate Professor and Asst. Director, Bhagwant Institute of Technology, Muzaffarnagar. He has been involved in various research activities. He has more than twenty papers in his credit which have been published in various international / national journals and refereed conferences. He has taught variety of new subjects and attended many workshops and conferences that are relevant to the field of genetic algorithms, software engineering, automated generation of test data, object oriented systems evolutionary computing etc. he is an active member of IEEE.