International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Algorithm Feasibility on IoT Devices with Memory and Computational Power Constraints

Anusha Medavaka

Software Programmer, Seven Hills IT Solutions LLC, NJ, India

Abstract: ***Internet of Things is a subject of much interest as well as, in last couple of years, safety of the IoT systems is a field of remarkable research activities. Shared verification between IoT devices as well as IoT web servers is a fundamental part of secure IoT systems. Solitary password-based verification mechanisms, which are commonly used, are vulnerable to side-channel and also dictionary attacks. In this paper, we present a multi-key (or multi-password) based shared verification device. In our strategy, the common key in between the IoT server as well as the IoT device is called protected vault, which is a collection of equal sized tricks. First components of the safe vault are shared in between the web server as well as the IoT device and components of the safe and secure vault modification after every successful communication session. We have implemented this device on an Arduino device to confirm our algorithm is practical on IoT devices with memory as well as computational power constraints.***

Keyword: IoT Device Authentication, IoT Security, Secure Vault

1. Introduction

On the planet of the Internet of Things (IoT), billions of devices are connected to the Internet, which provides an intruder a chance to adjust the IoT system on a large scale. Verification, consent, personal privacy as well as information privacy are a few of the significant safety concerns of IoT [9] Attacks on IoT devices can take place at one or more layers from the following: 1) Equipment layer, 2) Network layer and 3) Cloud layer [10] At the hardware layer, an assailant gets accessibility to the IoT hardware and also retrieves the keys or safety and security criteria stored inside the IoT device. The enemy can recreate a duplicate or virtual IoT device making use of the stolen safety specifications. The duplicate IoT device can publish false data to the server as well as get safe and secure details about the user from the server or the network to which the IoT device is linked. There are some side channels Attacks available utilizing which an opponent can get access to security criteria of the IoT device without having a physical accessibility to the device. Scientists have displayed electro-magnetic based side network Attacks to swipe secrets of RSA and ECC based file encryption [11,12] Using side network attacks AES encryption secrets can be taken from IoT devices [13,21] Because the IoT devices are linked to the internet, such devices are prone to Attacks with the network. MIRAI malware is an instance of such Attacks, where several IoT devices have actually been struck beyond the network and also utilized as network zombies to Attack various other web sites and also internet services [22] Peraković, et al. [16] have reviewed the enhanced quantity of DDoS attacks utilizing IoT devices. DDoS assaults based upon procedures like SSDP (a global plug and also play protocol), which is extensively utilized in IoT devices, have actually enhanced significantly after 2013. There have been various other situations of network Attacks where the assailant assaulted IoT devices from outdoors and also secondhand IoT devices to collect personal details of the owners1. An IoT device with an appropriate verification system can stay clear of numerous such circumstances. Scientists have been servicing producing such safe verification systems. These verification devices securely identify the web server and the IoT device using either a public trick or a common crucial infrastructure. In this paper, we propose a protected authentication method to authenticate the IoT device as well as the server. Some of the existing authentication systems, which are mainly based on single password-based device, are susceptible to side-channel and thesaurus Attacks. We have designed a multi essential authentication device, such that, even if the secret key (or a mix of tricks) made use of for recurring verification is fetched effectively by the enemy, the assailant cannot access to the extra verification keys as well as the verification system is protected from the side network assault or similar attacks. The vital values maintain transforming over the time, which prevents thesaurus attacks. This paper is organized as adheres to. We review previous work in Section 2. Section 3 describes system style and threat version. Our authentication mechanism is described in Area 4. Section 5 explains application details followed by Area 6, which gives efficiency analysis.

2. Previous Work

Lots of devices that become part of IoT system have constraints (such as computational, memory, energy, etc). IEFT's RFC 7228 [24] has suggested an application layer procedure, CoAP for low end IoT devices to attach to the internet. IEFT has actually also presented low power protection device, DTLS (Datagram Transport Layer Safety) [25] for protected communication over the CoAP method. Kothmayr et. al. [1] has proposed a two-way authentication system over the DTLS. The verification system is based upon the popular RSA plan, which is hard to deploy in drastically constricted devices. Raza, et. al. [2] likewise offer a technique based on the DTLS. They have adopted a common key method instead of RSA that makes it extra viable for resource-constrained devices. One method suggested by researchers for IoT verification is using ECC public vital file encryption [3] despite the fact that ECC requires much less memory and computational power than various other public key encryption techniques; it needs more memory and computational power than shared essential security. Likewise, some side channel assaults are feasible for ECC [4] Barreto et al. [5] present an SSO based authentication system for

confirming the IoT device, the IoT cloud and the user. They create a verification system where the server authenticates the user utilizing a user credential and after that the web server connects with the IoT device (they equally authenticate each various other). After both end factors (IoT device as well as the server) effectively confirm each various other, the server gives gain access to. Porambage, et al. [15] presented an ECC based two phase authentication formula. The plan of Porambage, et al. is a prevalent verification system based upon the ECC certificate. Butun, et al. [19] existing an end to end cloud driven authentication system for the IoT devices. They utilize ECC for authentication of the individual to the IoT device. The entire above authentication devices make use of ECC based public certificate or ECC based Diffie and Heilman system for verification, which makes the verification device safe and secure.

Jan et al. [6] presents a robust authentication mechanism utilizing which the web server as well as the IoT device can equally validate each other. They use shared vital technique to verify the server and the IoT device as well as a secret is shared between them. Their algorithm makes use of AES encryption for shared authentication. If this solitary key is lost (or jeopardized), both end points have to replace their shared tricks.

3. System Architecture

Figure 1 highlights a normal IoT system. The system contains 3 significant parts: An IoT device, an IoT web server and also an interface. The IoT device is accountable for gathering the data generated by the sensors attached to it as well as publishing them to the web server. Oftentimes, it also processes the data prior to submitting to the server. The IoT device interacts with the IoT server via a wide location network. This IoT system comes to the individual making use of a web and/or a mobile interface. Keep your text and visuals files separate up until after the message has been formatted as well as styled. Do not make use of hard tabs, and limit use of difficult returns to only one return at the end of a paragraph. Do not include any type of type of pagination anywhere in the paper. Do not number message heads-the design template will do that for you.

Assumptions

- We use a first safe consisting of n tricks of m bits each. Parameters m and also n can be chosen by the designer based on security requirements as well as memory constraints.
- IoT devices are constricted devices as well as have low memory, computational abilities as well as reduced energy accessibility.
- Each IoT device has a unique.

Recognition number appointed

- A preliminary secure vault is stored in the IoT device and also this initial safe is shared with the web server.
- The web server has a well-protected database.
- Side-channel assaults can be performed by an opponent.

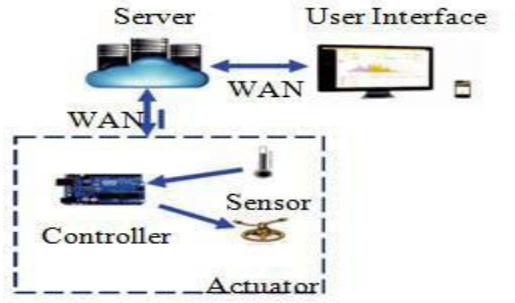

Figure 1 IoT System Architecture

Threat Model

The IoT web server is deployed in the cloud and also connects with the client (or IoT device) over WAN. Solitary essential based verification devices are not adequate to authenticate the IoT device to the web server. There are some side-channel assaults feasible to recover the shared secret throughout the communication between the IoT web server and the IoT device. If the password does not change over the moment, it is vulnerable to the thesaurus assault. When the opponent has the shared secret, a fake device can be created making use of that shared key. In our procedure, we make use of a collection of tricks, called a safe safe, to confirm both the web server and also the IoT device. This secure vault is initially shared in between the server as well as the IoT device and also it transforms its worth's based upon information traded in between the IoT server and also the IoT device. Therefore, contents of the vault change frequently. No extra message is exchanged in between the IoT web server and the IoT device to alter the worth of the secure vault. We use the conventional 3-way common verification for confirming the IoT web server as well as the IoT device. The communication is launched by IoT device by sending a link request to the server. When this request is obtained by the IoT web server, it returns a challenge to the IoT device; the IoT device replies to the IoT server's challenge and sends a verification obstacle to the IoT web server. The IoT web server verifies the reaction and also, if it is valid, the web server responds back to the IoT device's challenge. During the verification stage, the IoT server and also the IoT device establish a common key, called a session key. This session secret is used for 2 objectives. First, it is utilized to encrypt the messages exchanged in between the server and the IoT device. It is additionally utilized as an encryption trick for the message authentication code, which is utilized for message authentication. All the messages traded between 2 authentications thought about as a session. The session trick stays unchanged throughout a single session, but various sessions make use of different session tricks.

4. Authentication System

a) Secure Vault

The protected safe contains n secrets each trick being m bits long. The value of m is the crucial dimension. We denote all the keys as K [0], K [1], K [2], ..., K [n-1] while of deployment of the IoT device, the safe is shared in between the IoT device and the server. On the IoT device, the safe and secure safe must be stored in an encrypted style. On the web server, safe and secure vaults are saved in a safe and secure database.

b) Challenge-Response Mechanism

Our method utilizes a version of the well- recognized three-way authentication mechanism to mutually authenticate the IoT web server as well as the IoT device. Figure 2 represents the messages exchanged between the web server and also the IoT device. The IoT device initiates the procedure by sending the demand message M1 to the server. The demand message contains the unique id of the IoT device as well as a session id to maintain the authentication session. This message does not consist of any type of delicate details as well as, the message is not secured. The server validates the one-of-a-kind id of requesting IoT device as well as, if the message has the valid unique id, the web server sends back an obstacle message M2 to the IoT device. The challenge message contains a difficulty C1 and also a random number r1. C1 is a collection of p distinct numbers, and also each number stands for an index of a key, kept in the secure vault. C1 is represented as. The worth of p must be less than n.

M2 =

The values had in C1 are in between 0 as well as n-1. Once again, each aspect in C1 represents an index of a crucial saved in the safe and secure vault. The IoT device creates the action as follows: First, it generates a momentary vital k1 of dimension m little bits by doing XOR procedure on all the secrets whose indices are in C1. Thus, k1 = K [c11] K [c12] K [c1p] The IoT device produces the response for the difficulty by carrying out common vital security on r1|| t1 making use of k1 as the security trick. Note that|| is the concatenation procedure and Right here, t1 is a random number generated by the IoT device, which is better made use of to produce a session vital t. This session secret will be utilized for succeeding communication (as well as succeeding interaction is past the extent of this paper). The IoT device additionally generates a different challenge for the web server making use of the exact same mechanism. The IoT device produces a challenge C2, another set of p distinct arbitrary numbers, each number being in between 0 as well as n-1 as well as arbitrary number r2. Establish C1 and C2 are different. If C1 and C2 are very same, an assaulter can obtain the essential used for the C1 obstacle, as well as he can reuse that key for C2. The IoT device concatenates both the feedback and the difficulty for the web server as well as sends it back to the web server.

Message from the IoT device to the Server: M3 = Enc (k1, r1||) Where,

Enc: shared vital security

k1 = P [c11] P [c12] P [c1p] is the secret for the file encryption

C2 = c21, c22, ..., c2p

r2 = arbitrary number for the C2 obstacle

t1 = random number for session key generation. Once the server obtains the message M3, the server decrypts the message sent by the IoT device by producing the essential k1 from its safe vault. If the server gets r1 from the obtained message, it creates a reaction to the difficulty C2.The message sent out by the server back to the IoT device is:

M4 = Enc (k2, r2)

Where, k2 = P [c21] P [c22] P [c2p] and also k2 secret for the security

t2 = random number for session vital generation

The IoT device obtains the message M4 and also it verifies the identity of the server by returning the value of r2 by decrypting the message M4 making use of k2. When the server and also the IoT device verify each various other, they pick a session vital t = t1 and also all the additional interaction for this session is securely secured utilizing this session secret.

1) Man in the center assault

The man-in-the- center can record all the messages traded between the server and also the IoT device utilizing network spoofing. After spoofing all the messages exchanged for the authentication, it can identify itself as the web server to the IoT device and as the IoT device to the web server. In our method, we are using a session key t to confirm all the messages traded after verification. This session vital t is generated making use of two different random numbers t1 and also t2, which are traded in between the server and the IoT device in encrypted messages. The trick for those encrypted messages is a part of the safe safe, which is privately shared between the web server and the IoT device. Hence, the male-in-the-middle cannot fetch session crucial t from the messages exchanged between the web server as well as the IoT device, so the man-in- the-middle cannot get or modify any messages traded between the web server and the IoT device after the authentication.

2) Next password forecast

After every successful session, the IoT device and the web server alter the worths of the safe based on the data traded in between them. The brand-new worth of the secure vault must be arbitrary from the previous vault worth. If some passwords from a safe vault are predicted/retrieved by the enemy, the enemy must not able to forecast any other password of the next safe safe. We will certainly prove that the next password forecast is not feasible making use of random oracle version.

In the arbitrary oracle model, hash features are assumed as random oracles. A random oracle has adhering to residential properties:

- It takes an input x as well as generates an arbitrary

Result y.

- For every different worth of x, it produces

At various value y.

- Each time input x is offered to the arbitrary oracle, it generates the very same outcome y.

Therefore, all the outputs offered by the arbitrary oracle are random and also from the outcome supplied by the random oracle, it is not viable to predict the input. When producing a brand-new secure safe, initially we take the keyed hash (HMAC) of previous secure safe with the data traded between them as the secret. The arbitrary oracle produces a new arbitrary value, every single time a secure vault worth is supplied to it. This recently produced random value is cored with the previous safe worth's. According to the one-time pad theory, if we xor any type of worth with a random worth, the created output value will certainly be arbitrary. Thus, the recently produced safe worth's are random from previous worth's as well as the assaulter cannot forecast any worth of next oracle even if enemy understands a component of previous protected vault.

3) Side Channel Attack

Some side network attacks exist in well- known common vital security. For example, side network assaults based upon

power evaluation, temperature level analysis as well as memory evaluation can damage AES [13,21] for the single password based verification system; the assaulter can get the AES file encryption key associated with the obstacle-response making use of the side network Attack. In our method, the AES security trick is the combination of several tricks xored with each various other and it is not possible to obtain back those tricks from the file encryption trick. There is no chance an aggressor can recognize values of the tricks associated with the verification by just knowing the security trick. For this reason, it is not possible to get the whole secure vault from the side channel attack and also produce a replicate IoT device or infuse a false message to the network.

4) DoS Attack
An enemy can either flooding the web server or the IoT device with a lot of fake demands and also crash it as a result of source restraint. In our architecture, we are not assigning any type of resource prior to the authentication, so DoS attack is not feasible.

5. Performance Analysis

We did power and also safety evaluation for our algorithm. We compared our formula with ECC (Elliptic Curve Cryptography) based public essential encryption device and a straightforward 3-way authentication device with transforming tricks after every effective information exchange using power intake as the comparison measure. ECC is a light weight public crucial encryption plan usually made use of for IoT devices.

Power Evaluation
We utilized the approach described by Prasithsangaree, et. al. [20] to determine the power usage. Their technique stipulates that the overall power consumed is the product of ordinary existing attracted by the equipment, voltage offered to the hardware and the average time taken by the algorithm to perform. Arduino uses 19.9 mA of typical existing when provided with 5V voltage. We have actually evaluated the ordinary time for different formulas to determine the energy eaten by them.

Our formula needs one AES encryption and also one AES decryption at the IoT device side. For altering the secure vault worth, one HMAC operation is called for. So, the complete energy consumed by our procedure is 646.75 uJ. If we contrast our formula with ECC based verification, the energy intake is rather reduced. The most basic variation of verification with one password and AES-128 security calls for 2 AES procedures and it eats 497.5 uJ of power. Solitary rotating password-based system needs 3 AES operations, first 2 AES operation for authentication as well as the last one for the trading new password making use of previous password as security key. The complete power consumed by solitary rotating passwords is 746.25 uJ. Number 3 reveals the comparison between various authentication systems.

Security Evaluation
In this safety and security evaluation we think that an attacker can retrieve the password being made use of throughout the authentication mechanism making use of a side-channel attack. We contrast password forecast complexity for different values of m and also n, where m = variety of type in the safe as well as n = size of each key. Solitary turning as well as non-rotating based password techniques can be thought about as m = 1. For the authentication system with m = 1, the assaulter can obtain the actual password utilized for the verification utilizing a side network assault. For m = 2, the assailant needs to do brute force 2n hash procedures to recover both the passwords. In general, for a safe and secure vault with m keys (m > each having n bits calls for (m-- 1) * 2n strength hash procedures to anticipate the whole safe and secure safe. Table 4 shows the contrast of information memory called for and also password prediction complexity for different worth's of m and also n.

6. Conclusion

In this paper, we offered a system to provide a safe verification mechanism between the server and also the IoT device. Our formula is protected against side network assaults made use of to breach the protection of the IoT devices. The collection of passwords is changed after every successful session between the server and the IoT device. We make use of the fact that the IoT session entails numerous information exchanges and also this traded information is utilized to change the vault contents.

References

[1] Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., & Carle, G. (2012, October). A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication. In Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on (pp. 956- 963).IEEE.
[2] 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.
[3] Kalra, S., & Sood, S. K. (2015). Secure authentication scheme for IoT and cloud servers. Pervasive and Mobile Computing, 24,210-223.
[4] Danger, J. L., Guilley, S., Hoogvorst, P., Murdica, C., & Naccache, D. (2013). A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards. Journal of Cryptographic Engineering, 3(4), 241- 265.
[5] Barreto, L., Celesti, A., Villari, M., Fazio, M., & Puliafito, A. (2015, August). Anauthentication model for IoT clouds. In Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015 (pp. 1032-1035). ACM.[6]Jan, M. A.,
[6] Nanda, P., He, X., Tan, Z., & Liu, R. P. (2014, September). A robust authentication scheme for observing resources in the internet of things environment. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on (pp. 205- 211). IEEE.
[7] Gai, K., Qiu, M., Xiong, Z. and Liu, M., 2018. Privacy-preserving multi- channel communication in Edge-of-Things. Future Generation Computer Systems, 85, pp.190-200
[8] Gai, K. and Qiu, M., 2017. Blend arithmetic operations on tensor-based fully homomorphic encryption over real

numbers. IEEE Transactions on Industrial Informatics
[9] Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., & Bouabdallah, A. (2013, May). A systemic approach for IoT security. In Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on (pp. 351-355). IEEE.
[10] Suresh Kumar Mandala, Neelima Gurrapu, Mahipal Reddy Pulyala, " A Study on the Development of Machine Learing in Health Analysis", Indian Journal of Public Health Research & Development, volume 9, Number 12, December 2018, [ISSN-0976-0245(Print)-ISSN-0976-5506 (Electronic)]
[11] Suresh Kumar Mandala,Mahipal Reddy Pulyala and Sanjay Pachouri, "Being a Smart Sapien with Information Centric Networking and Cloud Computing", International Journal of Pure and Applied Mathematics,Volume 117, No. 21, 2017, 243-255,[ISSN: 1311-8080 (printed version)]
[12] Suresh Kumar Mandala,Sanjay Pachouri,"performance evaluation of multi stage attacks prediction",Journal of Advanced Research in Dynamical and Control Systems, Vol. 9, September 2017, JARDCS Special Issue On Engineering Technology.
[13] Thota Mounika, Mandala Suresh kumar,"Document Proximity: Keyword Query Suggestion Based On User Location",International Journal of Research,Volume 04, Issue 14, November 2017, [e-ISSN: 2348-6848 ,p-ISSN: 2348-795X].
[14] Syeda Sobia Farees , M. Suresh Kumar, "A Novel Approach for Protecting Location Information in Geosocial Applications ", IJIEMR, Vol 1, Issue 2, November2016 [ISSN:2456-5083]
[15] Suresh Kumar Mandala,Sanjay Pachouri, "A Reviewed Study on Financial Cyber Crime and Frauds", International Journal of Advances in Arts, Sciences and Engineering(ijoaase.com), Volume 4 Issue 9,Sep 2016, [ISSN. 2320-6144 (Online)]
[16] Siripuri Kiran, Ajmera Rajesh, "A Study on Mining Top Utility Itemsets In A Single Phase" in "International Journal for Science and Advance Research in Technology (IJSART)", Volume-4, Issue-2, February-2018, 637-642, [ISSN(ONLINE): 2395-1052]
[17] Yeshwanth Rao Bhandayker, "Security Mechanisms for Providing Security tothe Network" in "International Journal of Information Technology and Management", Vol. 12, Issue No. 1, February-2017, [ISSN : 2249-4510]
[18] Sugandhi Maheshwaram, S. Shoban Babu, "An Overview towards the Techniques of Data Mining" in "RESEARCH REVIEW International Journal of Multidisciplinary", Volume-04, Issue-02, February-2019 [ISSN : 2455-3085]
[19] Yeshwanth Rao Bhandayker , "A Study on the Research Challenges and Trends of Cloud Computing" in "RESEARCH REVIEW International Journal of Multidisciplinary ", Volume-04, Issue-02, February-2019 [ISSN : 2455-3085]
[20] Sriramoju Ajay Babu, Dr. S. Shoban Babu, "Improving Quality of Content Based Image Retrieval with Graph Based Ranking" in "International Journal of Research and Applications", Volume 1, Issue 1,Jan-Mar 2014 [ISSN : 2349-0020]
[21] Dr. Shoban Babu Sriramoju, Ramesh Gadde, "A Ranking Model Framework for Multiple Vertical Search Domains" in "International Journal of Research and Applications" Vol 1, Issue 1,Jan-Mar 2014 [ISSN : 2349-0020].
[22] Mounika Reddy, Avula Deepak, Ekkati Kalyani Dharavath, Kranthi Gande, Shoban Sriramoju, "Risk-Aware Response Answer for Mitigating Painter Routing Attacks" in "International Journal of Information Technology and Management", Volume VI, Issue I, Feb 2014 [ISSN : 2249-4510]
[23] Sugandhi Maheshwaram, "A Review on Deep Convolutional Neural Network and its Applications" in "International Journal of Advanced Research in Computer and Communication Engineering", Vol. 8, Issue No. 2, February-2019 [ISSN : 2278-1021], DOI 10.17148/IJARCCE.2019.8230
[24] Yeshwanth Rao Bhandayker. "An Overview : Security Solutions for Cloud Environment." International Journal for Scientific Research and Development 7.2 (2019): 1596-1598.
[25] Yeshwanth Rao Bhandayker. "AN OVERIEW OF CYBER SECURITY", International Journal of Research, vol. 8, Issue. 3 (2019): 2236-6124.
[26] Sugandhi Maheshwaram,"A STUDY ON THE CHALLENGES IN HANDLINGBIG DATA", International Journal of Research, vol. 8, Issue. 3 (2019): 2236-6124.
[27] Yeshwanth Rao Bhandayker. "An Overview of Service Models and Cloud Computing Evolution in IT",International Journal of Research and Applications,vol. 5, Issue. 20, Oct - Dec 2018 Transactions 5(20): 1000-1004. [ISSN : 2349 – 0020]
[28] Yeshwanth Rao Bhandayker. "A Comprehensive Survey on Security Issues and Advantages towardsCloud Computing",International Journal of Research and Applications,vol. 5, Issue. 18,Apr - Jun 2018 Transactions 5(18): 801-807. [ISSN : 2349 – 0020]
[29] Sugandhi Maheshwaram, . "A Study on Security Information and Event Management (SIEM)",International Journal of Research and Applications,vol. 5, Issue. 17, Jan - Mar 2018 Transactions 5(17): 705-708. [ISSN : 2349 – 0020]
[30] Sugandhi Maheshwaram, . "A Novel Technique for Preventing the SQL Injection Vulnerabilities",International Journal of Research and Applications,vol. 5, Issue. 19, July - Sep 2018 Transactions 5(19): 901-909. [ISSN : 2349 – 0020]
[31] Shoban Babu Sriramoju, "Substantial Overall Performance Pattern-matching Algorithm for Network Stability",International Journal of Research and Applications,vol. 5, Issue. 17, Jan - Mar 2018 Transactions 5(17): 701-704. [ISSN : 2349 – 0020]
[32] Sugandhi Maheshwaram. "A Study Design of Big Data by Concentrating on the Atmospheric Information Evaluation." International Journal for Scientific Research and Development 7.3 (2019): 233-236.
[33] Suresh Kumar Mandala,Sanjay Pachouri, "Analytical Study for Intrusion Detection System to Detect Cyber Attack",Airo International Research Journal, Volume VII, March 2016]ISSN: 2320-3714]
[34] Ranjeeth kumar.M,M.Suresh Kumar,S.S.V.N Sarma,"FUZZY KEYWORD SEARCH IN XML DATA",International Journal of Scientific &

Engineering Research, Volume 4,Issue 6, June2013 [ISSN:2229-5518]

[35] Yeshwanth Rao Bhandayker, "AN OVERVIEW OF THEINTEGRATION OF ALL DATA MINING AT CLOUD-COMPUTING" in "Airo International Research Journal", Volume XVI, June 2018 [ISSN : 2320-3714]

[36] Siripuri Kiran, 'Decision Tree Analysis Tool with the Design Approach of Probability Density Function towards Uncertain Data Classification', International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X,Volume 4 Issue 2, pp.829-831, January-February 2018. URL : http://ijsrst.com/IJSRST1841198

[37] Yeshwanth Rao Bhandayker , "Artificial Intelligence and Big Data for ComputerCyber Security Systems" in "Journal of Advances in Science and Technology", Vol. 12, Issue No. 24, November-2016 [ISSN : 2230-9659]

[38] Sugandhi Maheshwaram, "A Comprehensive Review on theImplementation of Big Data Solutions" in "International Journal of Information Technology and Management", Vol. XI, Issue No. XVII, November-2016 [ISSN : 2249-4510]

[39] Ajmera Rajesh, Siripuri Kiran, "Anomaly Detection Using Data Mining Techniques in Social Networking" in "International Journal for Research in Applied Science and Engineering Technology", Volume-6, Issue-II, February 2018, 1268-1272 [ISSN : 2321-9653], www.ijraset.com

[40] Sugandhi Maheshwaram, "An Overview of Open Research Issues in BigData Analytics" in "Journal of Advances in Science and Technology", Vol. 14, Issue No. 2, September-2017 [ISSN : 2230-9659]