International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 03, 2021

Anamoly Detection Using Pso In Cloud Integrated Iot Devices Usign Mdgan

M.Sumathi[1], N.G.S.Parameswaran[2]

[1]*Associate Professor, Department of Computer Science, Sri Meenakshi Govt. Arts College for Women, Madurai, Tamilnadu, India*
[2]*Assistant Professor, Department of Computer Applications, VHNSN College, (Autonomous), Virudhunagar, Tamilnadu, India*

Email: [1]sumathivasagam@gmail.com,[2]parames@eswardhas.pro

Abstract:The major impact of IoT functionalities primary depend on its cloud architecture. Though both these technologies executes in parallel but differs based on its principles and its functionalities. The device demand request is quenched using cloud methodologies as the resources are dynamic in nature. The access and demand are adopted for every resource and deploys cloud SPI architecture as the resources works on all the three verticals of cloud. The dynamic functionality is done without human intervention and are carried out by the basic principles of IoT. Due to this there is an urge for setting vigorous security mechanism in cloud and IoT to detect its anomalies. The launch of 2PA in this work implies security measures over IoT devices that get connect with the cloud for resource access. Both grant and access mechanisms are done with 2PA methods for providing immense security features for anomaly detection. The impact of PSO in this work provides optimization value for every IoT resources and the results are evaluated by MDGAN algorithm for providing optimized results.

Keywords: IoT, Resource Access, Two phase authentication (2PA), IoT Security, MDGAN, PSO

1. INTRODUCTION

One of key features of IoT is the resource allocation and its transactions. Steps to taken for ensuring secure transaction over un-trusted networks needs more observation for detecting anomalies. Cloud architecture are proven to be more secure and in our earlier work also addresses the same for providing secure solution for cloud transactions and its approach. As there is a technology drift for introducing the concept of IoT over cloud networks, more security measures need to undergone to balance the secure breeches between the IoT and cloud. The basic functionalities of cloud and IoT are resource grant and access to make transaction not become vulnerable to threats.

The introduction of Smart Grids (SG) makes the two communications to connect both IoT with the cloud using its sensors. The sensor gains the functionalities of grant and access mechanism to test its connection with the cloud using its sensors. The cloud utility service is activated that ensures the basic secure connection principles of integrity and confidentiality. Despite launching the basic secure mechanism the devices are not free from vulnerable threats. The connection between IoT devices with the cloud are done by SG hence the secure mechanism is applied to SG.

The 2PA authentication is applied to SG for both of its basic functionalities of grant and revoke that includes basic authentications and as well as biometric authentication to ensure maximum security measures. Such authentication does not adapt to basic cloud SLA hence 2PA is applied to every IoT devices.
The concept of 2PA implies more secure measures for providing both grant and revoke mechanism that uses secure mechanism with key management. The phase 1 uses basis authentication processes that uses PKY and are often changes dynamically based on resource access. It is followed by phase 2 where key is used for accessing the resources. Hence grant mechanism is done by Phase 1 and revoke mechanism is implied in Phase 2 for secure device access.

SURVEY

Xiao et al addresses the role of IoT for enhancing security techniques using machine learning. The concepts uses Artificial intelligence techniques for accessing device based on need. The observation of this work declares the importance of AI in IoT machine learning.
The work of Subburaj V and Chitra K, defines the new secure frame for launching PSO to detect vulnerabilities in mobile sensor. Since PSO works for sensor then the same can be adapted for IoT sensors too to detect anomalies with PSO optimized value.
Amin et. al, explains the concept of distributed cloud computing environment uses light weight protocols enabling IoT based devices. Distributed environment is the key concept to be addressed in IoT enabled platform for enhancing security in every devices connected to IoT environment.
Wang et.al, explains the concept of security with RFID tags by using ultra light weight authentication protocol. The protocol supports efficient means of communication that's acts efficiently for resource access.
He, Weijia, et al addresses HIoT along with efficient access mechanism implementing valid authentications. The rethinking and access information addressed in this work forecast on single user access mechanism that gets connected with multiple user mechanism. The work also emphasis of user location based accessed for getting linked with the resources.
The concept of decentralized mechanism is addressed with the bubbles of trust to justify the need of device identification and authentication is addressed by Hammi et.al. In order to justify the need of device management and access control the concept of deep learning is addressed by Das et.al, that portraits the need for authentication in device authentications.
A user authentication scheme of IoT devices using blockchain-enabled fog nodes is addressed by Almadhoun et.al justifies device identification along with user authentication. The device authentication of IoT device and its server uses secure vaults using Shah, Trusit et.al. In extend the work justifies device authentication and service implemented in different kinds of networks.

EXISTING MODEL

The traditional authentication process of SG is classified based on its accessibility. The general authentication method uses password mechanism that provides secure mechanism between transactions. The next level of approach is the authentication for devices. The span of password last only for moment and it will refreshed timely as the transactions differs based on time. Such approaches are adapted only for user authentication and it's viable to attacks. The problem becomes more fringed when low level user authentications are set.

On the other hand, hardware approach validates the user and creates a secure connection between the user and devices. The user level authentication after successful validation moves on to device level authentication as the devices uses validated encrypted methods to validate both uses and their interaction with the devices during the transactional process. This scheme is adapted to all devices that have in-build secure mechanism.

Such authentication reflects on multi level authenticity and provides secure access between the user and the devices. The device level authentication has the basic bio metric authentication that includes finger, eye, voice and other enhanced mechanism to provide strong and secure bond between user and devices.

The encryption standard adopted for user and device are done with symmetric key mechanism and its approach. The symmetric key uses hash function to provide various other encryption standards but primarily uses Asymmetric standards. These standard posses both certificate and no certificate secure standards for enhancing secure mechanism over IoT devices.

PROPOSED METHOD

The concept of 2PA is adapted in the proposed work as the secure mechanism is adapted for every IoT devices to execute grant and revoke mechanisms. The secure mechanism is implemented in its gateway and sets security trust between various IoT devices. The SG integrates various IoT devices using standard encryption standards with end to end secure mechanisms. Hence the basic functionalities of grant and revoke process are secured using security features with SG along with end to end secure process.

The configurations of SG are portrayed in the Fig 1 and enhance the basic secure mechanism over IoT devices and its sensors are shown. The SG interconnects all IoT devices and the security standards of SG are adopted by all the IoT devices. Both the authentication and the authorization are done by SG. Generally every devies should be recognized by its ID and are posted with the secure mechanism individually. When the security standards are adopted to SG all the devices mutually shared the security standard and finally every device are secured from the malicious attacks.

The Fig 2 and Fig 3 shows the interconnection of IoT devices with SG along with its authentication schemes to validate its process that includes both authentication and authorization. The extensive secure model is shown in Fig 3 that uses 2PA security phases.

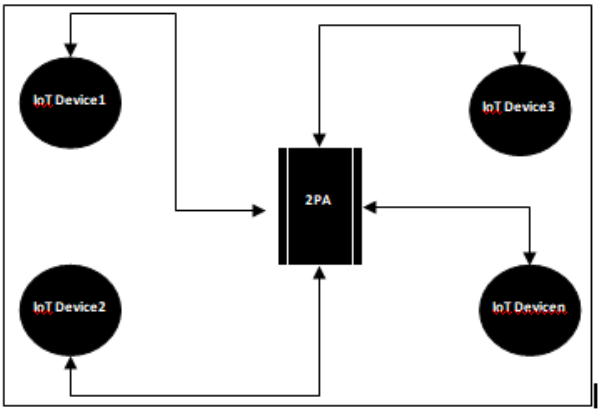

Fig 2: IoT device connectivity 2FA

The light weighed secure features that are adopted by all IoT devices interlinked with SG is shown in Fig 2. As the adoptions of secure features are extended to every device the

scheme is considered to be light weighted. The scheme adapts to both authentication and authorization. Both authentication and authorization were shown in Fig 4 and Fig 5 respectively.

Phase 1

The phase 1 to 2PA implies authentication as its first choice where users are given more credentials for their secure connection establishment with IoT devices. The below equation authenticated user with the term U and devices are with IoT_d. The extension of this phase is the password authentications that are represented as PWD that connects every user with the device.

$$R_i = \sum_{i=1}^{n} \sum_{j=i}^{m} (U_{i,j} IoTD_{i,j}) \quad (1)$$

$$IoTD_i = \sum_{i=1}^{n} (U_i PWD_i) \quad (2)$$

Phase 1: Device Registration

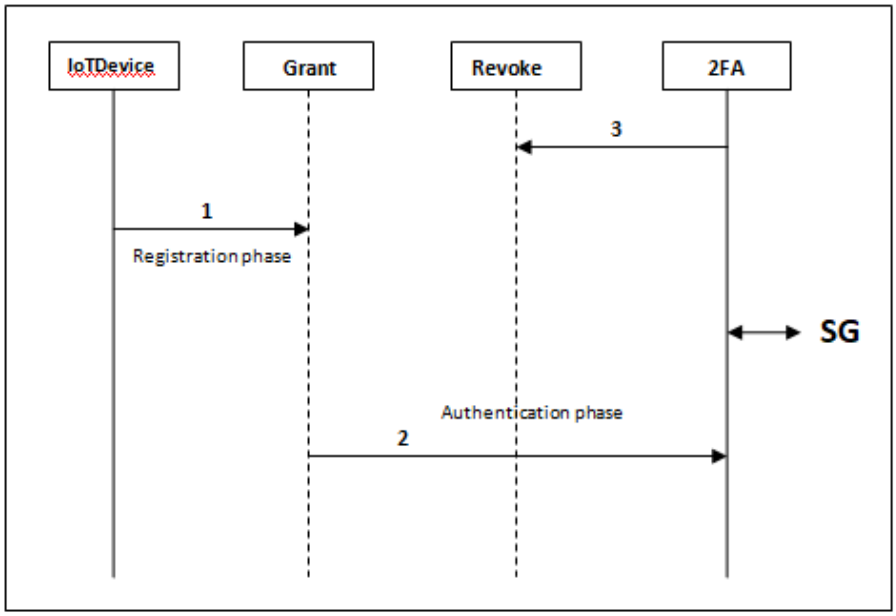

Fig 3: Device authentication phase – Grant

When R_i balances $IoTD_i$ with the U_i and PWD_i, then the device is successfully registered. The process is repeated for all the IoT devices getting connected into the system. The next phase is the authentication phase where every device is linked with SG when the initial phase is successful. When both the system and the password is validated it's registered into SG.

R is the resource that ranges from 'i' to N and the security schemes are set for all the resource that falls within the range. The extension of this phase makes the user connects with the devices as authorization phase and when both process gets validated then the devices are linked with SG.

IoT Device Grant

Step 1: Connection established for IoT devices with authentication process
Step 2: Authentication process is validated with Grant when its success
Step 3: Failure leads to Revoke mechanism

Phase 2

International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 03, 2021

The next phase is authorization where every device gets validated using revoke mechanism. It works with devices registration, devices initialization and device verification.

IoT Device Revoke

Step 1: Device registration after anomaly detection
Step 2: Once breech found, its Revoked
Step 3: When Success, the IoT device is Linked to SG

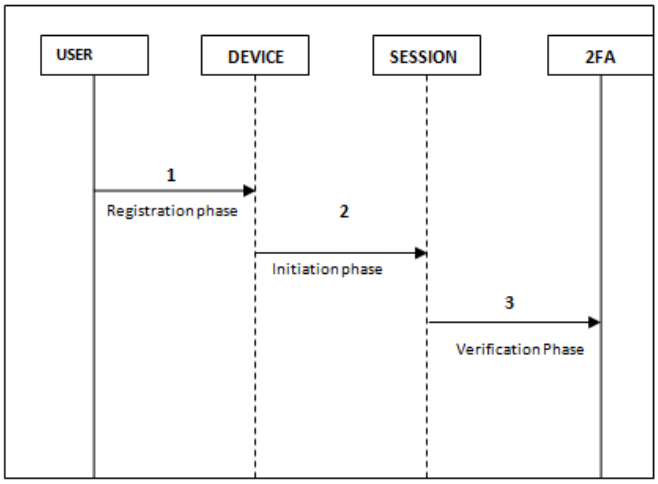

Fig 4: Anomaly IoT device detection

PSO OPTIMIZATION

Fitness function for grant and revoke IoT devies

$$Fitness(n) = {}^{a}/_{A} \quad (5)$$

Here in these formulae 'a' is the attack and A is the overall security breaches. The classification of attack is to ensure secure connection for applying PSO optimized value for every IoT devices to free from attacks.

This optimized value is set over IoT devices for both of its Grant and revoke process. The Grant acts as verification process over IoT devices and passes the optimized value to revoke process when the security measures fails. The failure is measured with the PSO optimized value.

The gateway verification phase were described by

Grant optimization process

$$\pi(i,j) \leftarrow \eta(i) + \eta(j)/2 \quad (6)$$

Revoke optimization process

$$\sigma(i,j) \leftarrow h(i) \times \pi(i,j) \quad (7)$$

MDGAN OVER IoT DEVICES

All the IoT devices interlinked with SG used MDGAN parameter to detect anomaly with its two evaluating parameter set as Grant and Revoke. Both Grant and Revoke receives different sample of optimized results and the results are subject to PSO for effective validation.

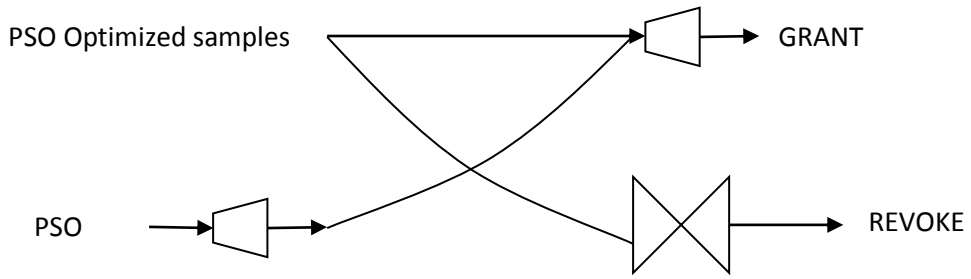

Fig 5: MDGAN PSO Optimization

2. RESULTS

The authentication process with its Grant mechanism is shown in Fig 6. The variable analysis is done with the SG by increasing the devices dynamically are shown in the graph. The device Id recognizes all the devices of SG and sets the authentication level.

IOT DEVICE OVERHEAD ANALYSIS

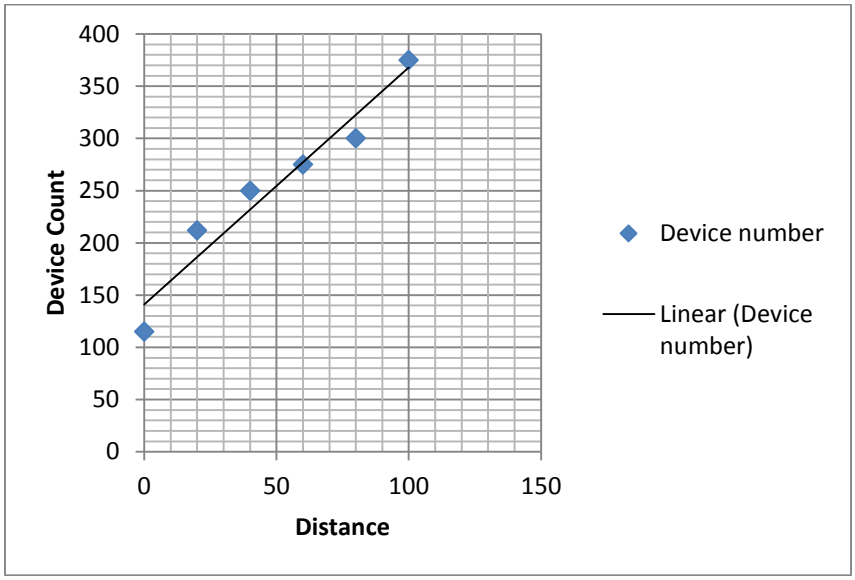

Fig 6: IoT devices Overhead analysis

Fig 7 shows the number of connected IoT devices within SG based on authenticity level check and its accessibility with the SG parameter.

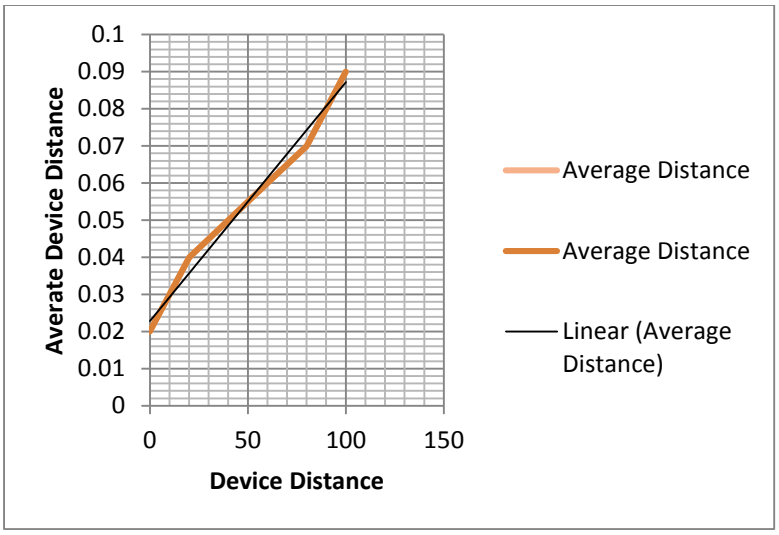

Fig 7: Average IoT devices with SG Zone

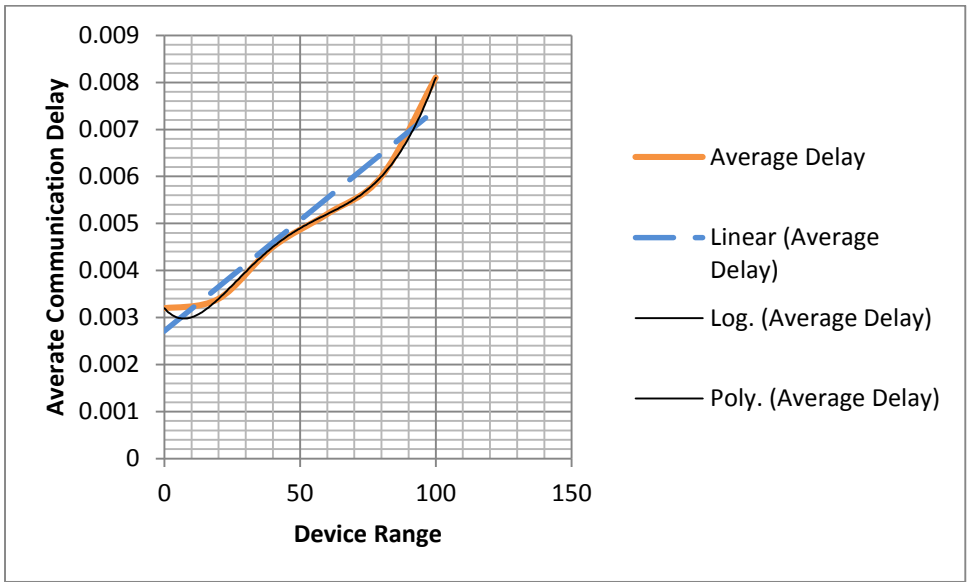

Fig 8: Average Delay in Communication overhead

Fig 9 evaluates the delay measure as delays are the main reason behind communication failures that is due to attack. Hence the delays have to be minimized for extended versatile security over IoT devices.

3. CONCLUSIONS

The work addresses the implication of 2PA authentication process for enhancing security measures for both cloud and IoT devices. The concept also implements PSO and MDGAN for setting device optimization and two phase authentication process measures using MDGAN. The results finally reduce the time delay in overall communication that resist between SG and its IoT connected devices. In extension the work will tends to increase the IoT devices dynamically to check the efficiency of the proposed approach.

4. REFERENCES

[1] Xiao, Liang, et al. "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?." *IEEE Signal Processing Magazine* 35.5 (2018): 41-49.
[2] Subburaj V and Chitra K, "Mobile Node Dynamism using Particle Swarm Optimization to fight against Vulnerability Exploitations", International Journal of Computer Applications (0975 – 8887), Volume 41– No.13, March 2012
[3] Amin, Ruhul, et al. "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment." *Future Generation Computer Systems* 78 (2018): 1005-1019.
[4] Wang, King-Hang, et al. "On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags." *The Journal of Supercomputing* 74.1 (2018): 65-70.
[5] He, Weijia, et al. "Rethinking access control and authentication for the home internet of things (IoT)." *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 2018.
[6] Hammi, Mohamed Tahar, et al. "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT." *Computers & Security* 78 (2018): 126-142.
[7] Das, Rajshekhar, et al. "A deep learning approach to IoT authentication." *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018.
[8] Almadhoun, Randa, et al. "A user authentication scheme of IoT devices using blockchain-enabled fog nodes." *2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA)*. IEEE, 2018.
[9] Kumari, Saru, et al. "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers." *The Journal of Supercomputing* 74.12 (2018): 6428-6453.
[10] Shah, Trusit, and Subbarayan Venkatesan. "Authentication of IoT device and IoT server using secure vaults." *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018.
[11] Tao, Ming, et al. "AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks." *Journal of Parallel and Distributed Computing* 118 (2018): 107-117.
[12] Braeken, An. "PUF based authentication protocol for IoT." *Symmetry* 10.8 (2018): 352.
[13] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." *Future Generation Computer Systems* 82 (2018): 395-411.
[14] Puthal, Deepak, and Saraju P. Mohanty. "Proof of authentication: IoT-friendly blockchains." *IEEE Potentials* 38.1 (2018): 26-29.
[15] Chatterjee, Urbi, et al. "Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database." *IEEE transactions on dependable and secure computing* 16.3 (2018): 424-437.
[16] Almulhim, Maria, and Noor Zaman. "Proposing secure and lightweight authentication scheme for IoT based E-health applications." *2018 20th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2018.
[17] Li, Dongxing, et al. "A blockchain-based authentication and security mechanism for iot." *2018 27th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2018.

[18] Mishra, Dheerendra, et al. "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks." *Multimedia Tools and Applications* 77.14 (2018): 18295-18325.
[19] Conti, Mauro, et al. "Internet of Things security and forensics: Challenges and opportunities." (2018): 544-546.
[20] Aman, Muhammad Naveed, Mohamed Haroon Basheer, and Biplab Sikdar. "Two-factor authentication for IoT with location information." *IEEE Internet of Things Journal* 6.2 (2018): 3335-3351.
[21] Cho, Do-Eun, Sang-Soo Yeo, and Si-Jung Kim. "Authentication method for privacy protection in smart grid environment." *Journal of Applied Mathematics* 2014 (2014).