ISSN (Online): 2455-7838
SJIF Impact Factor : 6.093

EPRA International Journal of

Research & Development

(IJRD)

Monthly Peer Reviewed & Indexed International Online Journal

Volume: 4, Issue:4, April 2019

Published By
EPRA Publishing

SJIF Impact Factor: 6.093 Volume: 4 | Issue: 4 | April | 2019 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Peer Reviewed Journal

ENABLING SECURITY VALUES FOR IoT APPLICATIONS FROM VARIOUS CLOUD ATTACKS USING SOFT COMPUTING TECHNIQUES

Dr. R. Poorvadevi
Assistant Professor, CSE Department, SCSVMV University, Kanchipuram, T.N, India

ABSTRACT
The Internet of Things (IoT) is advancement for user groups those whoever heavily using the web sources and applications. IoT deployment has been widely adopted in the heterogeneous environment for enhancing the digital applications. Though, it will have a significant economic potential, but it also gives malicious actors an ever-expanding toolbox for cyber attacks. Intruder's entry and attacks ratio is increasing day-by-day. Physical and digital threats are increasing in different user regions tremendously. Application and process specific functions are used in the different IOT sensors. While using the services from the service provider end numbers of attacks are created by the intruders. IoT platform will provide the service level usages and application specific functional values to the client. However, securing the IoT applications is essential from the distinct cloud attacks by applying the technological process and components to solve the issue. The proposed system will brings solution for protecting the IoT applications.
KEYWORDS: *IOT deployment, Digital threats, Cloud server, Controller area network (CAN), IoT hatches.*

I. INTRODUCTION

In the scientific computing world, all the generic applications and processes are running in the different client level machines. All the edge networks will function under the controlled environment known as computing servers. The IoT is a platform to enables the large computation activities will be performed by using the distinct IoT sensors. Whenever there is a client request, user applications are executed in the user operative devices. IoT applications are providing much computing facility over the client network access. There will be an increasing attacks rate for both in physical and digital formats. The recent survey report, says that the cloud attacks are the major attacks in the IoT platform. So, it is essential to regulate and avoid the cloud attacks in the IoT access environments.

II. LITERATURE SURVEY

As per an author, Mario Frustaci et.al, "Evaluating critical security issues of the IOT works: Present and future challenges". This paper has proposed the concept of analyzing the critical security issues in the IoT platform for the future and present challenging issues. They have defined the control-specific access environment for the use level process.[1]

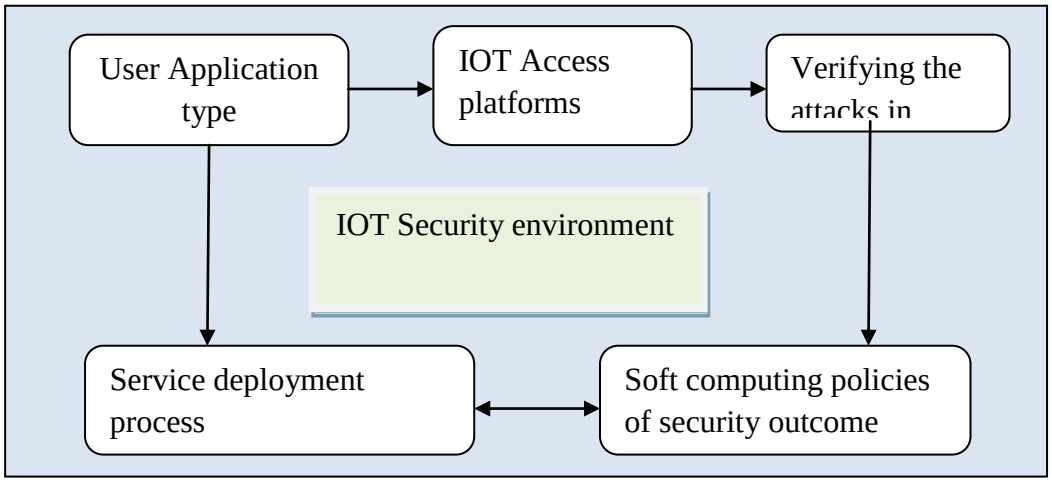
Author,"Asma Alsaidi et.al,"Security attacks and countermeasures on cloud assisted IoT applications". This paper gives the analysis outcomes of countermeasures on cloud assisted applications on the IoT platform. Various vulnerable are identified the novel framework was designed in the paper. [2]

As per an author, Biyut Mukherjee et.al, "End-to-End IoT security middleware for cloud-Fog communication". This paper has implemented the security middleware operations on the cloud fog communication by enabling the security principles in the digital threats. The key strategy of vulnerable finding for the security solution has evaluated on the hybrid cloud platforms. [3]

From the above study reports various attacks are monitored in the IoT platform with the countermeasures. But, no specific evidence and analysis reports for the cloud based attacks for the IoT applications were proved.

III. PROPOSED WORK

IoT platform has the major backbone applications for the user level applications to access the control system components from the authorized systems. The physical component was used in the IoT sensor to find the potential threats from the physical sensing and actuation of different set of sensors with the specific control systems. Physical layer will process the function of enhancing the security of unauthorized access to the physical sensing devices, actuation and its control systems. The CAN (controller area network) will initiate the program sequence of mobilizing all the physical components in the well protected manner. As both physical and digital threats increase, the need to find technologies to reduce such risks is also rising. This proposed work elaborates the solution to avoid vulnerable points in an IoT application and the key strategies to resolve them, including details on maintaining supply chain integrity.



The proposed work process (Fig 1) the schematic implementation at the security end for validating the user data. IoT service security has obtained in the various levels to enhance the secured transmission of user access information.

IV. IMPLEMENTATION WORK

During the process of service deployment time by the IoT app users and developers, they will be mitigating with the security constraints that can be used to verify the attacks rate form the cloud environment. To optimize the control factor for the IoT applications, the generic level service process can be initiated to produce the data security values on the client side platforms. The various service relevant attacks are monitored and investigated with the survey outcomes. The following are the recent attacks in the IoT service access environment.

- DDoS based Pure software attacks
- Network attacks
- Cryptanalysis attack
- Side-channel attack
- Data security
- Hardware security
- Block chain security

All the above attacks can be clearly analyzed with an internal process of botnets, Trojans and zombies. The various physical damages are notices in the various energy sources with the desired security level optimal solutions.

4.1 Importance of Soft computing Approach in IoT security Platform

The access level services are migrated with the security based control systems in order to optimize the supervisory control and software based attacks rate. Soft computing is the area where the user applications and services are well optimized with the certainty and uncertainty elements that are to be processed with the linguistic variables. All the general attacks can be classified in the following manner.

- Nature of user application
- Service process interval time

- Attacks deployment rate
- Kind of critical issue in security platform
- Access policy level information
- Sensor process over the cloud attacks
- Frequent cloud attack source details

All the above potential process can be isolated with the different types of attacks and the information level process on IoT sensor networks. The soft computing will establish the synchronized form of security principles in the cloud vendor and service process location.

The following are the computational formula that has been applied in the proposed work which is specified below:

IF the User data authorization is proved, THEN provide the service to the requested users

IF Generic services are processed THEN exploit the network level access constraints

IF IoT sensors processed in cloud platform THEM enhance the security value.

The above access constraints can be implemented on the service level trust worthiness to improve the security solution over the client access regions. The brute force attacks and Dos attacks also taken into consideration to prove the security value by increasing the strength of password combination to gain the access level information.

4.2 Enhancement of IoT security against the cloud attacks

The entire security based counterpart has been verified with the security essentials, like proving their service level genuineness, process segment over the service process, initiating the client level security values, proving the SCM access. All the Enterprises with IoT applications can achieve trustworthiness at each level of the supply chain, including people, process, design, and manufacturing and delivery levels. If there is a lack of information transfer at any link in the supply chain, it can enable security vulnerabilities and possibly open it up to a breach. Enterprise companies should have a policy in place to prevent unauthorized access to important systems while weeding out rogue vendors who could leverage technical loopholes to obtain sensitive data.

4.3 Enabling the IoT Security from Edge network to the Cloud Region

Enterprise companies need to ensure that their vendors and suppliers have defined Supply Chain Management (SCM) procedures that include baseline testing of components and specifications for parts used in IoT projects. In addition, they should be able to provide information on the entire manufacturing process. They should also share any changes in the system or any technical vulnerability in components with the IoT system owner. Any updates of the system such as changes in configuration, software changes and so forth should also be shared with the system owner or operator. Supply chain management systems should be able to consult a dashboard where they can easily access vendors' and suppliers' details, and any changes in the specifications of the components or parts.

V. EXPERIMENTAL RESULTS

All the IOT specific access platforms are heavily affected with attacks from various sources. However, there will be a plenty of attacks in the resource specific environment, cloud attacks are the major ratio which causing the attacks on the IoT service based platforms. All the network regions are computed with the service specific applications in order to process the security components by the authenticated and authorized person for sharing the resources. The following table shows the various security specific parameters are used in IoT with soft computing principles.

Table-1 Fuzzy Rule Implications for hybrid cloud services

Service ID in IoT platform	Edge device process status	Cloud attacks application with the soft computing process set	Desired security Process status
Region – 25.6	Migrated	Attack identified	Determined
Region Group-983-65-0	Processed	Fabricated	Processed
Region – 173-53-2	Optimized	IP spoofed data	Iterated
Region – 763-6-93	Processed	Enabled data source	Established

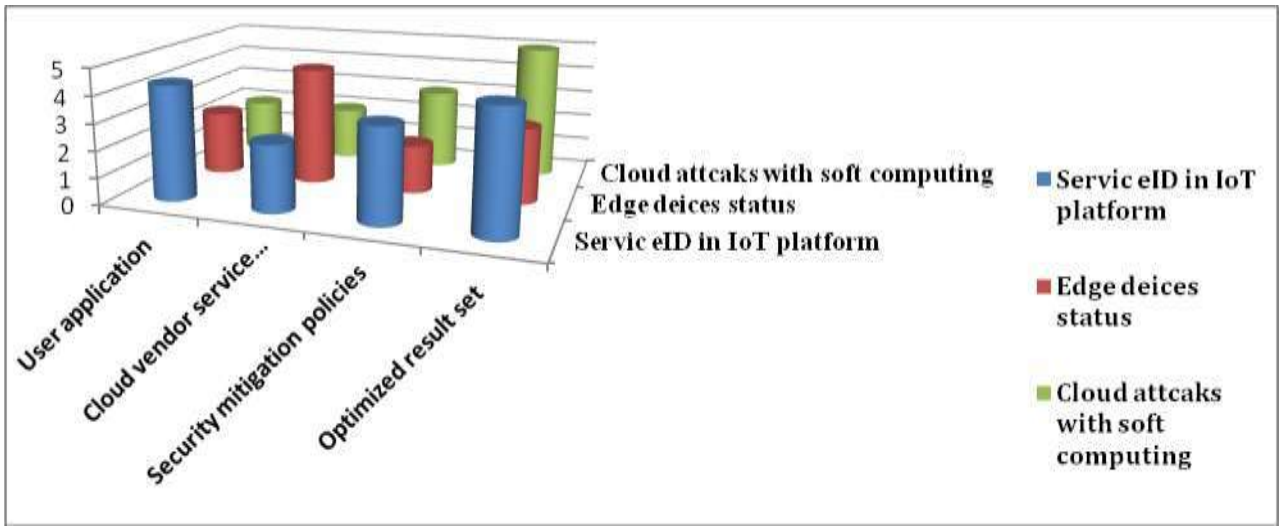


Fig:1 Illustration of Experimental outcomes

The above figure 1 and table 1 shows the functional operation components of IoT level data security in the various cloud attacks which has been deployed during the service development migration. All security generic processes are evaluated under various security parameters and specified their secured level of data process in the client platforms. The process depicts the process iteration levels based on the cloud attacks and its user application type. Entire process segments are used in the IoT platform to decide the attacks rate with the cloud vendor. Service level implementations are carried out in the security level policies. The IAM and SLA level verification are done in the client service access platform.

VI. CONCLUSION

In IoT service access environment, all the computational process are examined with the security level policies by integrating the security components and access specific constraints over the multi cloud platform attacks in the IoT environment. Applications are secured with user level access information and the soft computing rules are applied for the service optimization.

REFERENCES

1. *Mario Frustaci ; Pasquale Pace ; Gianluca Aloi ; Giancarlo Fortino , "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges", IEEE Internet of Things Journal , Volume: 5 , Issue: 4, Page s: 2483 – 2495, Year: 2018*
2. *Asma Alsaidi ; Firdous Kausar „ "Security Attacks and Countermeasures on Cloud Assisted IoT Applications", IEEE International Conference on Smart Cloud (SmartCloud), 2018*
3. *Bidyut Mukherjee ; Roshan Lal Neupane ; Prasad Calyam, "End-to-End IoT Security Middleware for Cloud-Fog Communication ",2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), Year: 2017*
4. *Avani Sharma ; Tarun Goyal ; Emmanuel S. Pilli ; Arka P. Mazumdar ; M. C. Govil ; R.C. Joshi, "A Secure Hybrid Cloud Enabled architecture for Internet of Things", IEEE 2nd World Forum on Internet of Things (WF-IoT),Year: 2015,Pages: 274 – 279, 2015*
5. *Ikuo Nakagawa ; Shinji Shimojo, "IoT Agent Platform Mechanism with Transparent Cloud Computing Framework for Improving IoT Security", 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC) , Volume: 2, Year: 2017*
6. *Sowmya Nagasimha Swamy ; Dipti Jadhav ; Nikita Kulkarni, "Security threats in the application layer in IOT applications ", 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017*
7. *Mohammad Aazam ; Imran Khan ; Aymen Abdullah Alsaffar ; Eui-Nam Huh, "Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved ", Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th - 18th January, 2014*
8. *Luciano Barreto ; Antonio Celesti ; Massimo Villari ; Maria Fazio ; Antonio Puliafito, "An authentication model for IoT clouds", 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2015*
9. *Anam Sajid ; Haider Abbas ; Kashif Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges", IEEE Access, Volume: 4, Year: 2016*