International Journal of Control and Automation
Vol. 13, No. 2s, (2020), pp. 235-243

# An Efficient Amalgamation of Computational Models to Ensure a Secure IoT Environment

Sachi Nandan mohanty[1], A.Radhika[2], Vandna Dahiya[3] Chinmaya Ranjan Pattanaik[4], Sujathakrishamoorthy[5]

*[1]Department of CSE,Faculty of Science and Technology,IFHE Hyderabad, India. [2]Department of Electrical and Electronics Engineering, Sri Krishna College of Engineering and Technology, Coimbatore. India[3]Department of Education, GNCT, Delhi, India,*
*[4]Computer Science and Engineering, Ajay Binay Institute of Technology, Cuttack, Odisha, India.*
*[5]Department of computer science, Wenzhou kean university, Zhejiang province, Wenzhou, China.*

***Abstract***

*The cloud computing merges with the IoT environments to enhance the scope of developing new applications and distributing these applications to the real world environment. But the current IoT environment faces many challenges in building an efficient IoT applications. In these challenges, ensuring security in the IoT environment plays a vital role.Traditional cloud models tried to solve the security issues in the IoT applications. But they all failed in producing the optimal solution. To solve the security issues of the IoT applications an amalgamation is performed between computing models such as cloud computing and corner society. The proposed system merges the trust examination model and usage template in which this combination solves the load balancing problem in the cloud computing. The corner environment structure which is made effectively and reducing the usage of the resources through the corner protocols to maximize the ability of the trust examination model. The proposed system gives the flexibility of loading the usage template in the cloud and loading the usage grammar template in the corner protocol in which results in the development of the IoT applications.*
***Keyword –*** *Internet of Things, Cloud Computing, Trust Examination Model, Security, Amalgamation.*

## 1. Introduction and Literature Survey

The interaction of electronic devices can be happened at anytime and anywhere through the concept of Internet of Things [1].In spite of various positive points are there in Internet of Things there are some negative points are also present in the Internet of Things such as security problems, lack of storage society and processing ability [2]. Cloud computing is an excellent technology will solve the issues such as lack of storage society and security undertaken by the Internet of Things environment, where cloud provides three services such as infrastructure as a service, platform as a service and software as a services. The IoT environment is combined with the cloud in which the components of Internet of Things are integrated in web [3].

As said earlier security problem plays a vital role in the performance of the Internet of Things application. The Internet of Things architecture consists of various layers in its structure. Various types of inner attacks will target the network layer and bottom layer which consists of various collections of processing components [4]. While speaking about the communication problem, waiting time increases in the environment when the Internet of Things environment and cloud service are at different location. The waiting time arise when the IoT components are far from the cloud service [5]. An efficient resource clustering algorithm was proposed to develop an efficient wireless personal cloud environment which leads to the advantages in the future internet of things [6].

The trust examination model and usage template developed in a corner based internet of things merged cloud environment is the proposed system which can solve the security and storage society problems of

ISSN: 2005-4297 IJCA

the research work. The network layer of the internet of things had been merged which provides the storage capacity through cloud computing [7]. The corner society consists of enormous collections of datacenters, systems under fog environment and various advantages in the services offered by the cloud such as makespan [8] [9]. An efficient job scheduling algorithm was proposed based on probability distribution to enhance the scheduling solution for the cloud environment [10].

The proposed system is sub divided into two ways as corner society and corner policy. The corner society is built on the existing deployed corner architecture and also included in the Internet of Things environment. The corner policy composes corner architectures that provides the procedure for combining IoT and Cloud in which it is implemented as a server cloud scheduling process for the proposed System [11]. The traditional systems implemented various trust examination architecture in which to address the problems caused by the inner attacks in the IoT environment [12]. The implementation of the trust examination architecture had various merits in many parameters such as merging the data transmission and mining and usage promising [13]. This method of merging the model of computation is given by corner architecture which addresses the problems faced by the IoT environment and produces the efficient usage [14].

Some of the blockchain systems develops the efficient security model of Internet of Things environment [15].An efficient metaheuristic approach was proposed improve the job scheduling solutions in the cloud environment [16]. This chapter describes the introduction and literature survey in most detail. The literature speaks about the internet of things, cloud computing, the combination of the cloud computing and the internet of things, corner policy and corner society or architecture. The coming chapters includes the composing the proposed system, results and discussions with the comparison results of both existing and proposed systems and conclusion of the current research work

## 3. Composing the Proposed System

The working of the components includes the narrow trust calculation and passes the exception to the corner society in the Internet of Things. The trust calculated points are attained and verified by the corner society for the entire trust domains of Internet of Things. The usage template is published in the cloud and the corner policy as these usage components template is located where it is present in the cloud to analyze the information and template methods. The trust examination model is merged along with the cloud computing and internet of things with the help of corner computation. At the time of internet of things usage concept publication, the trust examination model permits the corner policy to calculate the required trust components to generate or pass the data. It also includes the corner society which balances the load of the internet of things society.

For deploying the corner society to reduce the illegal communication in the trust examination model, through implementation it maintains the jobs in the internet of things and also works for the unique internet of things usage and ensures the data in a needed way. Due to this, the corner society or the architecture is an efficient option to the wireless internet of things. Probably needed or merge usage template are stored in the corner policy, which is flexible and works effectively for the internet of things in which it interacts with the maximum amount of resources. The maximum amount of trust examination model will be published in the corner policy which contains components defect clearing calculation, data error calculation and inner attack calculation at the level of information. Thus by implementing the corner society or architecture the latency is reduced and the identification of exceptions in the reduced price.

### 3.1 The Proposed Usage System

The usage system of the IoT merged cloud environment is divided into three stages. Each and every stages comprise a collection of procedures as layers. Content cluster layer, Content processing layer and user working usage layer. In this usage system, the content cluster layer is combined with the corner society, the content processing layer is combined with the corner protocols or policy and the user working

ISSN: 2005-4297 IJCA

usage layer comprises the top end as well as the opening end of the cloud environment. The corner society depicts various properties such as reloading the comments and unexpected trust, operates non static job scheduling in the IoT cum cloud environment by selecting the suitable trust resources which performs as trust layer on the entire IoT environment. Operating the unique requirements such as waiting time, flexibility and correctness. At the same time the corner society comprises some of the properties such as various virtual resources are mined from the hardware resources with the help of concept called virtualization. It also generates the template parameter and grammar template $Template_{parameter}$in the corner society.

The non static job scheduling methodology for the cloud environment is processed and this procedure is combined with the corner society to ensure the extensibility and easy management in operating the information in the IoT environment. Same procedure is to be followed to combine the corner society and corner protocol to extend the properties for calculating the grammar of the user requirements and identifying the related $Template_{parameter}$in the cloud environment, this should be performed before passing the optimal digital content to the receiver corner protocol or policy, combining with the corner protocol or policy to publish a various $Template_{parameter}$in which there will not be any related $Template_{parameter}$at that time and stores the various $Template_{parameter}$The usages having definite requirement are processed first when comparing to the other usages. For knowledge mining and future content prediction large number of heuristics contents are used for the processing.

### 3.2 Algorithm: Usage System

**Input: User's Requirements**

**Output:** $\boldsymbol{Array_{Solution}^{Corner-1}}, \boldsymbol{Array_{Cloud}^{Solution}}, \boldsymbol{Solution_{amalgamation}}$

$1. Rec \rightarrow Corner - 1;$

2. $Rec \xrightarrow{extract} Do(environment, boundary_{variable}, variety_{variable},,,,,, Variety_{usage});$
3. $Cluster \xrightarrow{digital\ format} Array_{variable} + Solution_{amalgamation};$
4. $Array_{variable} \xrightarrow{size} Size_{Array};$
5. **for** *i*from 1 to $Size_{Array}$ $\boldsymbol{do}$
6. **if** *Array[i]*∈ $Template_{parameter}$ and $Ur_{resource}$ in Corner – 1
7. **then**
8. Corner – 1 transfers $IN_{cloud}$ which is present in $Template_{parameter}$ to the associated edges;
9. Corners identify $Template_{parameter}$ based on $IN_{cloud}$ and processes it;
10. Corner produces the solutions to Corner – 1 and load these solutions
11. into $Array_{Solution}^{Edge-1}$;
12. **else**
13. Transfer *Array [i]* to the cloud;
14. **if** *Array [i]* ∈ $Template_{parameter}$ in cloud **then**
15. **if** $cloud.Ur_{time}^{sum} > Corner1.Ur_{time}^{sum}$and $Ur_{resource} == 1$ of Corner -1 **then**
16. The cloud transfers $IN_{cloud}$ in $Template_{parameter}$ to the associated target corners
17. Corners identify$Template_{parameter}$ based on $IN_{cloud}$ and processes it;
18. Corners produces the solutions to Corner – 1 and Corner – 1 load these solutions
19. into $Array_{Solution}^{Corner-1}$;
20. Corner – 1 renovate its $Template_{parameter}$ from the cloud;
21. **else**
22. The cloud transfers $IN_{cloud}$ in $Template_{parameter}$ to the associated target corners
23. Corners identify $Template_{parameter}$ based on $IN_{cloud}$ and processes it;

ISSN: 2005-4297 IJCA

Corners produces the solutions to cloud and the cloud load these solutions into
into $Array_{Solution}^{Corner-1}$;
**end if**
**else /***Develop different $Template_{parameter}$*/
The cloud verifies the configuration compatibility of corners and produces a different $Template_{parameter}$
The cloud transfers the syntax protocol and $Template_{parameter}$ to the associated destination corners and commands the corners to develop a different $Template_{parameter}$
Corners process the utilities with the help of Corner society
**if** $Cloud.Ur_{time}^{sum} > Corner_{time}^{sum}$ and $Ur_{resource} == 1$ of Corner $- 1$
**then** Corners produces the solutions to Corner – 1 and Corner – 1 load these solutions
into $Array_{Solution}^{Corner-1}$;
**else**
Corners produces the solutions to cloud
**end if**
**end if**
**end if**
**end for**

## 4. Results and Discussions

The results and discussion section deals about the results of the proposed system based on the parameters such as rate of components servers, relationship time and identification of inner attack affected components in percentage. This section also provides the comparison results for the processing systems such as depending on the corner society, depending on combination leader, common combination leader, with trust examination model and without trust examination model.

| **Depending on the Corner (DOC)** | | |
|---|---|---|
| **S.No** | **Rate of Component servers** | **Relationship Time in milliseconds** |
| 1. | 0.48561 | 6.0292 |
| 2. | 2.19137 | 7.74274 |
| 3. | 3.8631 | 9.74082 |
| 4. | 5.61946 | 11.5919 |

**Table 1. Rate of Component servers and their Relationship Time Depending on the Corner society**

ISSN: 2005-4297 IJCA

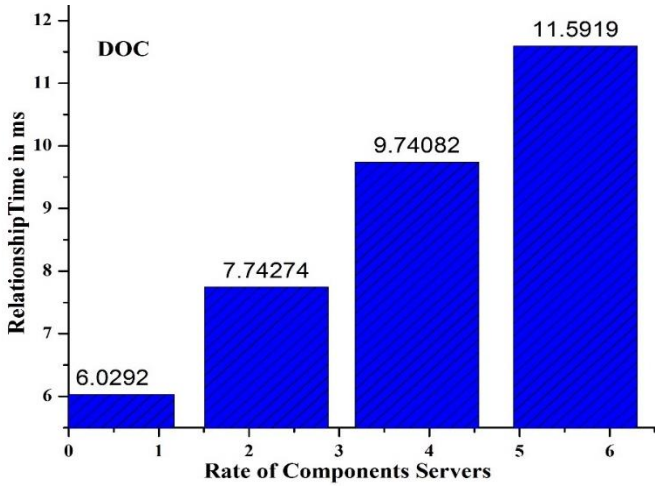


**Figure1. Relationship time Depending on the Corner society**

| Depending on Combination Leader (DOCL) | | |
|---|---|---|
| **S.No** | **Rate of Component servers** | **Relationship Time in milliseconds** |
| 1. | 0.88439 | 12.1195 |
| 2. | 2.56655 | 16.4362 |
| 3. | 4.26621 | 19.8948 |
| 4. | 5.99871 | 24.503 |

**Table 2. Rate of Component servers and their Relationship Time Depending on the Combination Leader**

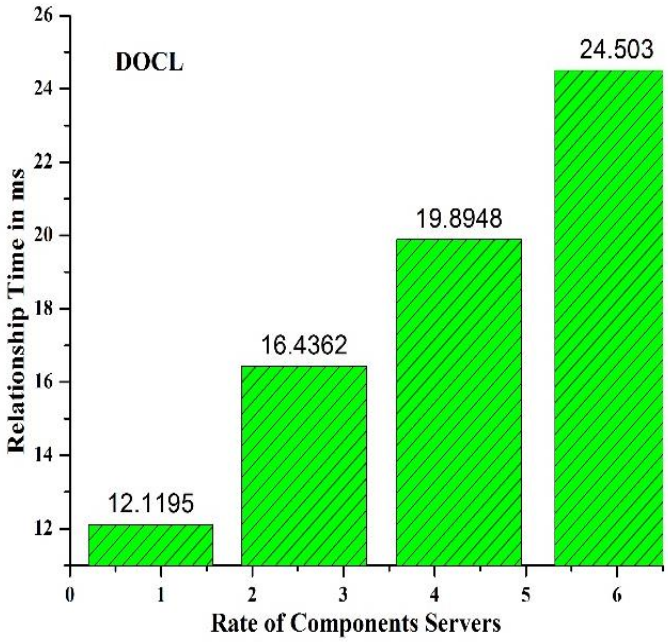


**Figure 2. Relationship time Depending on the Combination Leader**

Table 1 and figure 1 depicts the performance of the depending on the corner society. Table 2 and figure 2 depicts the performance of the depending on the combination leader approach. Table 3 and figure 3 depicts the performance of the common collection trust. These results produced based on the parameters of rate of components server and the relational time which is mentioned in milliseconds.

| Common Collection Trust | | |
|---|---|---|
| **S.No** | **Rate of Component servers** | **Relationship Time in milliseconds** |
| 1. | 1.28918 | 11.7282 |
| 2. | 2.93452 | 20.1975 |
| 3. | 4.62913 | 30.3913 |
| 4. | 6.35573 | 42.8811 |

**Table 3. Rate of Component servers and their Relationship Time Common Collection Trust**

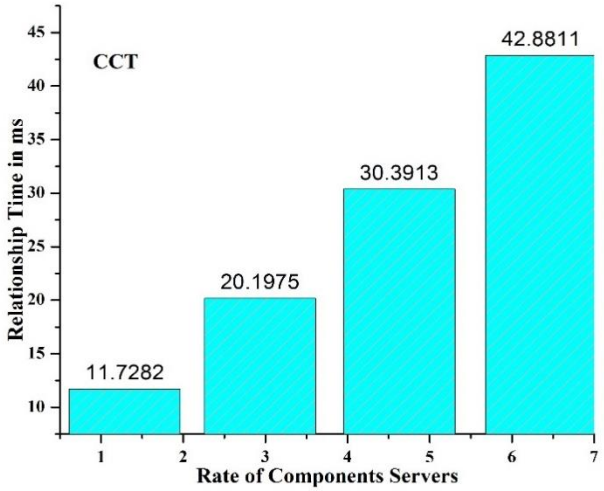


**Figure 3. Relationship time Depending on the Common Collection Trust**

| With Trust Examination Model | | |
|---|---|---|
| **S.No** | **% of Inner attack affected Components** | **Time in milliseconds** |
| 1. | 0.97938 | 5.95366 |
| 2. | 4.58763 | 7.18747 |
| 3. | 10.1031 | 8.81085 |
| 4. | 15.4124 | 10.3287 |
| 5. | 20.8763 | 11.8119 |
| 6. | 25.7216 | 13.1186 |
| 7. | 29.0722 | 14.0718 |

**Table 4. Inner attack affected Components Identified by with Trust Examination Model**

ISSN: 2005-4297 IJCA

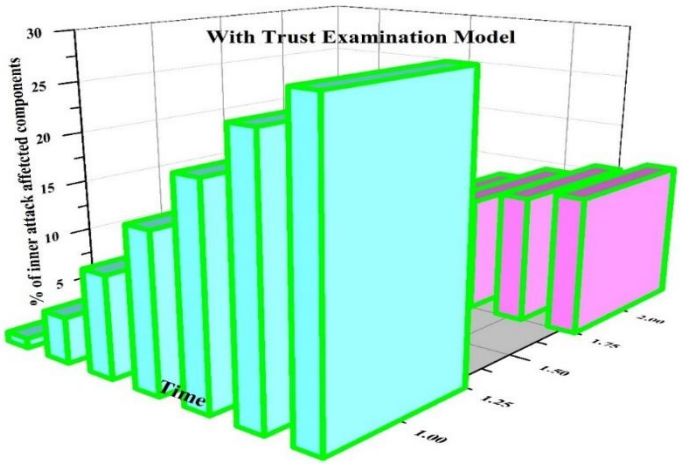


**Figure 4. Inner attack affected Components Identified by with Trust Examination Model**

| Without Trust Examination Model | | |
|---|---|---|
| **S.No** | **% of Inner attack affected Components** | **Time in milliseconds** |
| 1. | 1.13402 | 6.05906 |
| 2. | 5 | 6.03307 |
| 3. | 10.1031 | 6.36008 |
| 4. | 15.2062 | 7.10722 |
| 5. | 20 | 9.04401 |
| 6. | 25.1031 | 12.1019 |
| 7. | 29.0206 | 15.9622 |

**Table 5. Inner attack affected Components Identified by without Trust Examination Model**

The table 4 and figure 4 results depicts the performance of the with trust examination model. The table 5 and figure 5 results depicts the performance of the without trust examination model. Results are based on the parameter identification of inner attacks affected components in percentage.

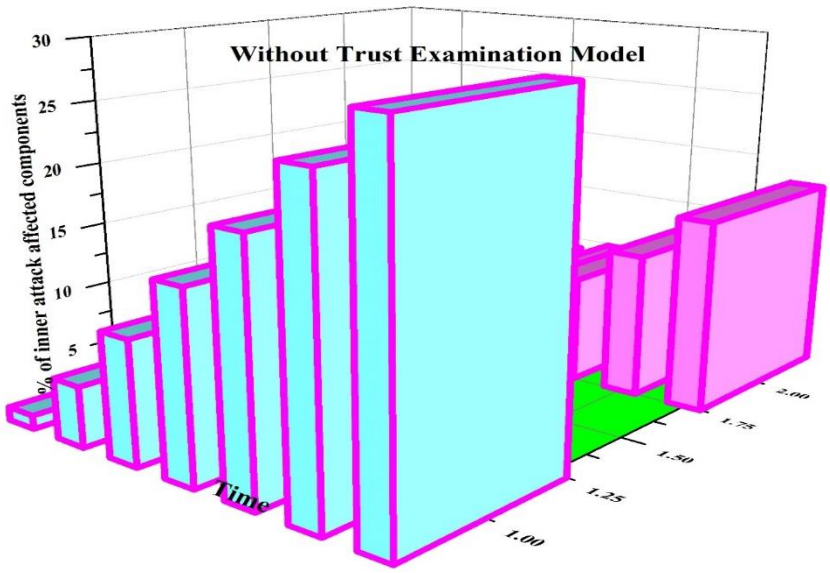


**Figure 5. Inner attack affected Components Identified by without Trust Examination Model**

ISSN: 2005-4297 IJCA

## 5. Conclusion

The results of the research work ensured the need of the Trust examination model in any internet of things application. The trust examination model identifies the percentage of inner attack affected components more than the system without the trust examination model. The corner society and usage template plays a vital role in helping these trust examination model to provide an efficient secure environment for the internet of things and cloud combined application. The amalgamation of the corner society, corner policy, usage template and cloud computing works well for the Internet of environment and produces the optimal solution. In the future a novel algorithm is planned to develop an efficient IoT – cloud environment.

## References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, andM. Ayyash, "Internet of things: A survey on enabling technologies, protocols,and applications," IEEE Communications Surveys and Tutorials,vol. 17, no. 4, pp. 2347–2376, 2015.
[2] A. Botta, W. D. Donato, and V. Persico, "Integration of cloud computingand internet of thingsa survey," Future Generation Computer Systems,vol. 56, pp. 684–700, 2016.
[3] J. Yang, C. Wang, Q. Zhao, B. Jiang, Z. Lv, and A. K. Sangaiah, "Marinesurveying and mapping system based on cloud computing and internetof things," Future Generation Computer Systems, vol. 85, pp. 39–50,2018.
[4] Praveen Sundar, P.V., Ranjith, D., Vinoth Kumar, V. et al. Low power area efficient adaptive FIR filter for hearing aids using distributed arithmetic architecture. Int J Speech Technol (2020). https://doi.org/10.1007/s10772-020-09686-y.
[5] Umamaheswaran, S., Lakshmanan, R., Vinothkumar, V. et al. New and robust composite micro structure descriptor (CMSD) for CBIR. International Journal of Speech Technology (2019), doi:10.1007/s10772-019-09663-0
[6] Karthikeyan, T., Sekaran, K., Ranjith, D., Vinoth kumar, V., Balajee, J.M. (2019) "Personalized Content Extraction and Text Classification Using Effective Web Scraping Techniques", International Journal of Web Portals (IJWP), 11(2), pp.41-52
[7] Vinoth Kumar, V., Arvind, K.S., Umamaheswaran, S., Suganya, K.S (2019), "Hierarchal Trust Certificate Distribution using Distributed CA in MANET", International Journal of Innovative Technology and Exploring Engineering, 8(10), pp. 2521-2524.
[8] Maithili, K , Vinothkumar, V, Latha, P (2018). "Analyzing the security mechanisms to prevent unauthorized access in cloud and network security" Journal of Computational and Theoretical Nanoscience, Vol.15, pp.2059-2063.
[9] T. Wang, G. Zhang, Z. A. Bhuiyan, A. Liu, W. Jia, andM. Xie, "A novel trust mechanism based on fog computing insensor-cloud system," Future Generation Computer Systems, 2018, https://doi.org/10.1016/j.future.2018.05.049.
[10] V.Vinoth Kumar, Ramamoorthy S (2017), "A Novel method of gateway selection to improve throughput performance in MANET", Journal of Advanced Research in Dynamical and Control Systems,9(Special Issue 16), pp. 420-432.
[11] Dhilip Kumar V, Vinoth Kumar V, Kandar D (2018), "Data Transmission Between Dedicated Short-Range Communication and WiMAX for Efficient Vehicular Communication" Journal of Computational and Theoretical Nanoscience, Vol.15, No.8, pp.2649-2654.
[12] Kouser, R.R., Manikandan, T., Kumar, V.V (2018), "Heart disease prediction system using artificial neural network, radial basis function and case based reasoning" Journal of Computational and Theoretical Nanoscience, 15, pp. 2810-2817.
[13] Shalini A, Jayasuruthi L, Vinoth Kumar V, "Voice Recognition Robot Control using Android Device" Journal of Computational and Theoretical Nanoscience, 15(6-7), pp. 2197-2201.
[14] B. Cheng, G. Solmaz, F. Cirillo, E. Kovacs, K. Terasawa, and A. Kitazawa,"Fogflow: Easy programming of iot services over cloud and edges for smart cities," IEEE Internet of Things Journal, vol. 5, no. 2,pp. 696–707, 2018.

ISSN: 2005-4297 IJCA

[15] Jayasuruthi L,Shalini A,Vinoth Kumar V.,(2018) " Application of rough set theory in data mining market analysis using rough sets data explorer" Journal of Computational and Theoretical Nanoscience, 15(6-7), pp. 2126-2130.
[16] M Kowsigan, S Rajkumar, P Seenivasan, C Vikram Kumar, "An Enhanced Job Scheduling in Cloud Environment using Improved Metaheuristic Approach", International Journal of Engineering Research & Technology, Vol 6, No 2, pp. 184-188, 2017.

ISSN: 2005-4297 IJCA