International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9553-9557

Novel Collaborative Intrusion Detection System (Ids) Method Based On Cloudlet Mesh

Divyavani G[1] and Dileep Kumar Reddy P [2]

[1]II year M.Tech SE Student, Computer Science and Engineering Department, JNTUACEA Ananthapuramu, India.

Assistant Professor (Adhoc), Computer Science and Engineering Department, JNTUACEA, Ananthapuramu, India.

Abstract

The recognition of wearable devices, at the side of the construction of muddles and perplex let telecommunications, there was accelerating ought to yield surpass hospital therapy. The processing enslave of preventive testimony principally consist of testimony assemblage, info stockpile and input distribution, etc. Traditional healthcare arrangement regularly calls for the birth of pharmaceutical input to the shower, and that comes to users' responsive info and causes conversation strength depletion. Practically, therapeutic picture allocation can be a very important and hard deliver. Thus during this essay, we building up a peculiar healthcare process by using the power of distract let. The functions of muddle let encompass retreat insurance, picture dividing and intervention unmasking. In entertainment industry of testimony assortment, we antecedent employ Number Theory Research Unit (NTRU) structure to cipher user's remains goods cool by wearable devices. Those inputs would be transmitted to within reach perplex let in an electricity valuable fit. Secondly, we show a new have confidence form to lend a hand user to pick out believable partners who desire to participate saved testimony within the perplex let. They believe form further lend a hands analogous patients to keep in touch near one another roughly their diseases. Thirdly, we shift users' preventive testimony saved in far off muddle of health center toward triplet's parts, and provide conservatives right kind safety. Finally, in order to offer protection to the healthcare technique starting with wicked attacks, we improve a innovative shared invasion disclosure arrangement (IDS) mode in accordance with perplex let coincide, that can dramatically save you the far off healthcare big info distort beginning at attacks. Our experiments describe the clout of one's scheduled scheme.

Keywords: Cloud-based Privacy Preservation, Evaluation of collaborative, Collaborative IDS Performance.

INTRODUCTION

With the advancement of medicinal services huge information and wearable innovation, and additionally distributed computing and correspondence advancements, cloud-helped human services enormous information registering ends up basic to meet clients' ever-growing requests on wellbeing interview. Be that as it may, it is testing issue to customize particular social insurance information for different clients in an advantageous mold. Past work recommended the blend of social systems and human services administration to encourage the hint of the infection treatment process for the recovery of real time malady data. Human services social stage, for example, Patients Like Me, can acquire data from other comparative patients through information partaking as far as client's own discoveries. Despite the fact that sharing medicinal information on the interpersonal organization is advantageous to both patients and specialists, the delicate information may be spilled or stolen, which causes protection and security issues without productive insurance for the mutual information. In this way, how to balance security assurance with the comfort of therapeutic information sharing turns into a testing issue. With the advances in distributed computing, a lot of information can be put away in different mists, including cloudlets furthermore, remote mists, encouraging information sharing and escalated calculations. Be that as it may, cloud-based information sharing involves the accompanying crucial issues:

- How to protect the security of user's body data during it delivery to a cloudlet?
- As can be predicted, with the proliferation of electronic medical records (EMR) and cloud-assisted applications, more and more attentions should be paid to the security problems regarding to a remote cloud containing healthcare big data. How to secure the healthcare big data stored in a remote cloud?
- How to effectively protect the whole system from malicious attacks?

As far as the above issues, this paper proposes a cloudlet based human services framework. The body information gathered by wearable gadgets are transmitted to the adjacent cloudlet. Those information are additionally conveyed to the remote cloud where specialists can access for sickness analysis. As indicated by information conveyance chain, we partitioned the security assurance into three phases. In the main stage, client's indispensable signs gathered by wearable gadgets are conveyed to a wardrobe passage of cloudlet. Amid this stage, information protection is the primary concern. In the second stage, client's information will be further conveyed toward remote cloud through cloudlets. A cloudlet is framed by a specific number of cell phones whose proprietors may require as well as offer some particular information substance. In this way, both security insurance and information sharing are considered in this stage. Particularly, we utilize trust model to assess confide in level between clients to decide

sharing information or not. Thinking about the clients' therapeutic information are put away in remote cloud, we order these medicinal information into various types and take the relating security approach. In expansion to over three phases based information security insurance, we likewise consider communitarian IDS in light of cloudlet work to secure the cloud biological community.

In rundown, the fundamental commitments of this paper include:

A cloudlet based medicinal services framework is displayed, where the security of clients' physiological information and the proficiency of information transmissions are our fundamental concern. We utilize NTRU for information assurance amid information transmissions to the cloudlet.

- keeping in mind the end goal to share information in the cloudlet, we utilize clients' similitude and notoriety to develop confide in display. Based on the deliberate clients' put stock in level, the framework decides regardless of whether information sharing is performed.
- We separate information in remote cloud into various types and use encryption component to secure them individually.
- We propose community oriented IDS in light of cloudlet work to ensure the entire social insurance framework against vindictive assaults.

RELATED WORK

Cloud-based Privacy Preservation

Regardless of the improvement of the cloud innovation and rise of more cloud information sharing stages, the mists have not been broadly used for medicinal services information sharing due to security concerns. There exist different deals with ordinary security insurance of health e care information. In Lu et al., a framework called SPOC, which remains for the safe what's more, protection saving shrewd registering system, was proposed to treat the capacity issue of social insurance information in a cloud condition and tended to the issue of security and security insurance under such a domain.

We proposed a compound determination which applies various joined innovations for the security insurance of medicinal services information sharing in the cloud condition. In Cao et al., a MRSE (multi keyword positioned seek over encoded information in distributed computing) security insurance framework was displayed, which plans to give clients with a multi-watchword strategy for the cloud's encoded information. Despite the fact that this strategy can give come about positioning, in which individuals are intrigued, the measure of computation could be lumbering. In Zhang et al., a need based wellbeing information total (PHDA) plot was exhibited to ensure and total diverse composes of social insurance date in cloud helped remote body region organize (WBANs). The article explores security and protection issues in portable human services networks, including the security insurance for social insurance information conglomeration, the security for information handling and trouble making. Portrays an adaptable security demonstrate particularly for information driven applications in distributed computing based situation to ensure information classification, information trustworthiness and fine grained get to control to the application information. give an efficient writing audit of security assurance in cloud-helped medicinal services framework.

PROPOSED SCHEME

Various earlier works have examined distinctive interruption location frameworks with very a few advances. For instance, proposed a conduct govern determination based system for interruption recognition. The primary commitment is the execution beats different strategies for irregularity based methods. Proposed a collective model for the cloud condition in light of circulated IDS and IPS (interruption counteractive action framework). This model makes utilization of a half breed discovery method to distinguish and take relating measures for any sorts of interruption which hurt the framework, particularly disseminated interruption. In any case, community IDS in view of the cloudlet work structure is another sort of interruption recognition strategy, which was first proposed in Shi et al. The creators showed that the identification rate of the interruption recognition framework built up based on a cloudlet work is generally high. portrays configuration space, assaults that sidestep CIDSs and assaults on the accessibility of the CIDSs, and presents correlation of particular CIDS approaches. Depicts the IDS for protection cloud. The creators give a diagram of interruption identification of distributed computing and give another plan to protection cloud security.

Table 1. Key Parameters Used in the CIDS

Variable	Explanation
Ii	Instrusion i
Ai	Alarm for IDS i
1-β	Detection Rate
α	False Alarm Rate
Ec	Expected Cost(Relative degree, no unit attached)
q1	Probability of Collaborative IDS Reporting an Alarm
q2	Probability of Collaborative IDS Reporting No-Alarm

Collaborative IDS In this section, collaborative IDS is designed among m IDS, e.t., S1, S2, · · · , Sm, in order to get higher detection rate and lower false alarm rate. The m IDS are assumed to detect independently. There exists K different types of intrusion. So according to deduce in the following, we can get the detection rate and false alarm rate of collaborative IDS. In order to evaluate it , we give the ROC curve. Before transmitting data to the remote cloud, we

establish the collaborative IDS based on the cloudlet mesh to complete the intrusion detection task.

We use {S1, S2, . . . , Sm} to represent the set of IDS's in the collaborative IDS (CIDS) system. Suppose that each IDS is able to detect intrusion independently. For the sake of simplicity, we use I to indicate that there is intrusion behavior in this system and *NI* to indicatethat there is no intrusion. Furthermore,*A* means that IDS raises an alarm while *NA* means no alarm.We use $1-\beta$ to indicate the detection rate and α as the false alarm rate. If there exists*K* different types of intrusion, denoted as *I*1, *I*2, . . . , *IK*, then we have $I = I1 \cup I2 \cdots \cup IK$. Assume that the probability of *Ij* is *pj* , *j* = 1, 2, . . . ,*K*. Therefore, the probability of intrusion behavior in this system is $p(I) = \Sigma K\ i{=}1\ pi$, while the probability of no intrusion behavior is $P(NI) = 1 - p(I)$.

We thus have that $p(A|I) = 1 - \beta$ and $p(A|NI) = \alpha$. As for each IDS, we use $p(NAi|Ij) = \beta ij$ to represent the probability of IDS *Si* not triggering an alarm when having *Ij* , and $p(Ai|NI) = \alpha i$ as the probability of *Si* triggering an alarm when not being attacked. It follows that

$$\beta = p(NA|I) = p(NA1|I) \cdots p(NAm|I). \quad (3)$$

Since $Ii \cap Ij = \phi$, $i \neq j$, applying the total probability formula, we can obtain the probability that system *S*1 does not trigger an alarm when there is an attack to intrude the system, as

$$p(NA1|I) = \frac{p(NA1 \cap (I1 \cup I2 \cdots \cup IK))}{P(I)}$$

$$= \sum_{j=1}^{k} \beta 1 \mathrm{j} \mathrm{Pj} / \sum_{j=1}^{k} \mathrm{Pi} \quad (4)$$

For system *Si*, *i* = 2, 3, . . . ,*m*, let $p(NAi|I)$ denote the probability

that no alarm is triggered by *Si*. We have

$$p(NA1|I) = \sum_{j=1}^{k} \beta 1 \mathrm{j} \mathrm{Pj} / \sum_{j=1}^{k} \mathrm{Pi} \quad (5)$$

We can derive β as follows.

$$\beta = \prod_{\mathrm{i}=1}^{\mathrm{m}} \sum\nolimits_{-}(j = 1)\text{^}k \blacksquare \beta 1 \mathrm{j} \mathrm{Pj}) \ / \ (\sum\nolimits_{-}(j = 1)\text{^}k \blacksquare \mathrm{Pi}) \quad (6)$$

The false alarm rate $\alpha = p(A|NI) = 1 - p(NA|NI)$ can be obtained in a similarly manner, as

$$p(NA1|I) = \prod_{\mathrm{i}=1}^{\mathrm{m}} (1 - \alpha \mathrm{i}) \quad (7)$$

We thus obtain the detection rate α and false alarm rate β of the collaborative IDS system. The corresponding ROC curve can be

Evaluation of collaborative

IDS We next consider the cost problem of collaborative IDS, with its cost being divided into three parts:

• When the intrusion behavior is not detected by the system, but IDS generates an alarm, the system will prevent the transmission of this user's data, which will affect the normal use of the healthcare system by the user, and may lead to decrease of the system's reliability. The cost at this moment is denoted as Cα;

• When the system suffers from intrusion Ii , 1 ≤i≤ K, but the IDS does not generate an alarm, the system will allow this intrusive behavior, which will break the healthcare big data; the healthcare data in the remote cloud is attacked and may probably cause leakage of

patients' data. The cost of this scenario is denoted as C˜ i , 1 ≤ i ≤ K;

• The cost in other scenarios is marked as 0. Without loss of generality, we define the cost rate as Ci = C˜ i/Cα. In the following, we adopt the decision tree to model the corresponding expected cost problem. Let q1, q2 = p(NA) denote the probability of no alarm in a system. Based on the total probability formula, we have

Without loss of generality, we define the cost rate as *Ci* =~ *Ci/C_*. In the following, we adopt the decision tree to model the corresponding expected cost problem. Let *q*1, *q*2 = *p*(*NA*) denote the probability of no alarm in a system. Based on the total probability formula, we have

$$q1 = (1 - \beta)\sum_{t=1}^{K} \mathrm{Pi} + \alpha(1 - \sum_{t=1}^{K} \mathrm{Pi}) \quad (9)$$

$$q2 = \beta \sum_{t=1}^{K} \mathrm{Pi} + (1 - \alpha)(1 - \sum_{t=1}^{K} \mathrm{Pi}) \quad (10)$$

Let $p1;i = p(Ii|A)$, *i* = 1, 2, . . . ,*K*, denote the probability of intrusion occurrence under the condition that the system fires an alarm. Thus, *p*1;*i* can be calculated as follows.

$$p1;i = \frac{(1 - \prod_{\mathrm{j}=1}^{\mathrm{m}} \beta ji)pi}{1 - \beta \sum_{t=1}^{K} \mathrm{Pi} + \alpha(1 - \sum_{t=1}^{K} \mathrm{Pi})} \quad ,i=1,2,3 \ldots\ldots K \quad (11)$$

Let $p1;K{+}1 = p(NI|A)$ denote the probability of no intrusion under the condition that the system fires an alarm, then:

$$p1,K{+}1 = 1 - \sum_{t=1}^{K} \frac{(1 - \prod_{\mathrm{j}=1}^{\mathrm{m}} \beta ji)pi}{1 - \beta \sum_{t=1}^{K} \mathrm{Pi} + \alpha(1 - \sum_{t=1}^{K} \mathrm{Pi})} \quad . (12)$$

Let $p2;i = p(Ii|NA)$, *i* = 1, 2, ·,*K*, denote the probability of intrusion occurrence when no alarm is given. It follows that

$$p2;i = \frac{\prod_{\mathrm{j}=1}^{\mathrm{m}} \beta jipi}{\beta \sum_{t=1}^{K} \mathrm{Pi} + \alpha(1 - \sum_{t=1}^{K} \mathrm{Pi})} \quad , \quad \mathrm{i}=1,2,3,\ldots.\mathrm{K} \quad (13)$$

Let $p2;K{+}1 = p(NI|NA)$ denote the probability of no intrusion occurrence when no alarm is given. We have

$$p2,K{+}1 = 1 - \sum_{t=1}^{K} \frac{\prod_{\mathrm{j}=1}^{\mathrm{m}} \beta jipi}{\beta \sum_{t=1}^{K} \mathrm{Pi} + \alpha(1 - \sum_{t=1}^{K} \mathrm{Pi})} \quad (14)$$

From the above analysis and the assumption on the cost rate, we can derive the expected cost as follows.

$$Ec = q1 \cdot p1,K{+}1 + q2 \ . \sum_{t=1}^{K} \mathrm{P2, j. Cj} \quad (15)$$

Now let's consider how to choose the optimal IDS numbers and IDS combinations when constructing the collaborative IDS system. Hereby we formulate an optimization problem based on the decision tree model. That is, under the circumstances of guaranteeing a certain detection rate $1 - \beta$˜ and false alarm rate α, we shall choose the optimal number m,

so that we can achieve the minimum expected cost. The formulated problem is given below.

minimize Ec (16)

subject to: $\alpha < \sim\alpha, \beta < \sim\beta$ (17)

$0 \leq pij \leq 1, i, j = 1, 2, \ldots, K$ (18)

$0 \leq qi \leq 1, i = 1, 2, \ldots, K$ (19)

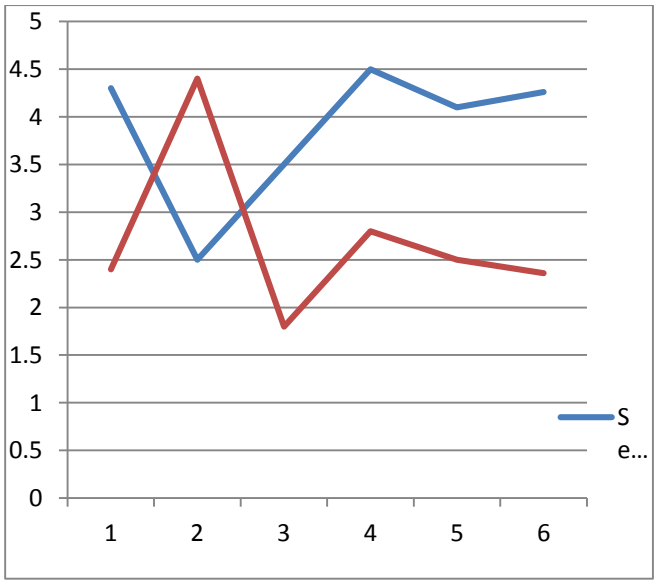
$Cj > 0, j = 1, 2, \ldots, K.$ (20)

We can select a certain number of IDS systems, in order to guarantee: (i) the detection rate ($1 - \beta \geq 1 - \beta\tilde{}$) is sufficiently large; (ii) the false alarm rate (α) is sufficiently small; and (iii) the expect cost of the entire system is minimized.

SIMULATION STUDY

Performance Discussion about data encryption

As discussed, we shall encrypt the data with the algorithm, which has been introduced previously, to protect private information after the data are collected by the users themselves. However, we also need to evaluate the performance of the proposed algorithm. We describe the changes of delivery ratio of client data encryption method with remote cloud encryption mechanism with the incensement of time. Fig. 3 shows the results. Through this figure, we can see two methods will both achieve a good delivery ratio with the incensement of time, while in general, the encryption method in remote cloud have better performance than encryption method at user end.

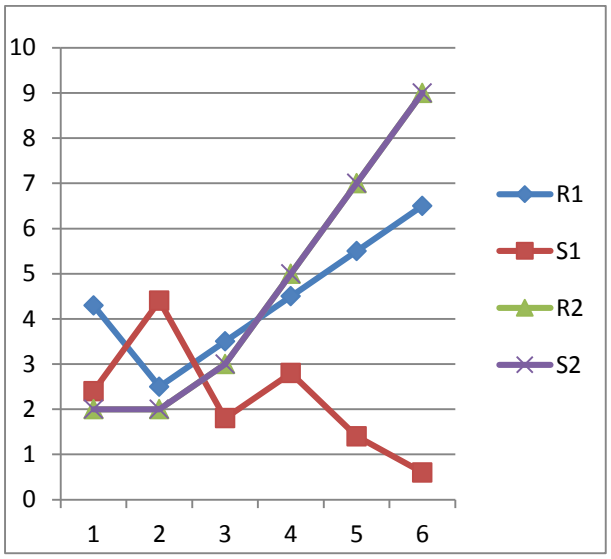


X-Axis: Time

Y-Axis: Delivery Ratio

Collaborative IDS Performance Results

We use the cloudlet mesh simulator to evaluate the effectiveness of the mesh security infrastructure. We develop IDS executed by multiple servers in the mesh. We use three independent IDS's and two intrusion types in our experiment. The probabilities of different types of intrusion are p1 = 0.001 and p2 = 0.0015. Figure 5 plots the detection rate in the ROC curve of various IDS's used in the experiment against the false alarm rate. According to Fig. 5, the detection rate of every single IDS is below 30%. However, the collaborative IDS can achieve a detection rate of 60%, which is a considerable improvement over the single IDS approach. If the IDS generate no alarm when there is actually an intrusion, the system would suffer heavy loss. Our proposed collaborative IDS perform well from this regard. Nevertheless, we want to minimize the cost in addition to achieving a high detection rate. We consider two cost measures: C1 = 5 and C2 = 6. The unit of the cost is not shown here, because only relative costs are compared. There are six Trust level IDS's in this experiment, whose operational parameters are given in Table 2. We assume baseline values α.



User Reputation

Figure: Comparison of the delivery ratio of the encryption method in the remote cloud and user end. and Comparison of the trust level.

Table 2. Detection Rates of Various IDS Schemes

Cloudlet	**αi**	**1-βi1**	**1-βi2**
Cloudlet 1	0.009	0.35	0.36
Cloudlet 2	0.008	0.34	0.35
Cloudlet 3	0.006	0.32	0.34
Cloudlet 4	0.005	0.3	0.32
Cloudlet 5	0.004	0.28	0.3
Cloudlet 6	0.002	0.26	0.28

If m = j, $1 \leq j \leq 6$, there are C j 6 choices, and the cost value m is chosen as the smallest cost among those C j 6 costs. We guarantee the detection rate to be above 70% and the false alarm rate to be below 3.5%. At the same time, we search for the lowest cost configuration for the collaborative IDS system. The theoretical derivation leads to the optimal solution. Because the detection rate of single IDS is below 35%, our collaborative system has doubled the detection rate at a minimum cost. It can be seen from Fig. 6 that four IDSs should be chosen to work collectively and cooperatively to yield the optimal performance

CONCLUSION AND FUTURE WORK

In this paper observed the problem of privacy protection and sharing large medical data in cloudlets and the remote cloud environments. We developed a system which does not allow users to transmit data to the remote cloud in consideration of secure collection of data, as well as low communication cost. However, it does allow users to transmit data to a cloudlet, which triggers the data sharing problem in the cloudlet

Firstly, we can utilize wearable devices to collect users' data, and in order to protect users privacy, we use NTRU mechanism to make sure the transmission of users' data to cloudlet in security. Secondly, for the purpose of sharing data in the cloudlet, we use trust model to measure users' trust level to judge whether to share data or not. Thirdly, for privacy-preserving of remote cloud data, we partition the data stored in the remote cloud and encrypt the data in different ways, so as to not just ensure data protection but also accelerate the efficacy of transmission. Finally, we propose collaborative IDS based on cloudlet mesh to protect the whole system. The proposed schemes are validated with simulations and experiment

REFERENCES

[1] H. Mahmud, A. M. Amin, M. E. Ali, and T. Hashem, "Shared execution of path queries on road networks," Clinical Orthopaedics Related Res., vol. abs/1210.6746, 2012.

[2] L. Zammit, M. Attard, and K. Scerri, "Bayesian hierarchical modelling of traffic flow - With application to Malta's road network," in Proc. Int. IEEE Conf. Intell. Transp. Syst., 2013, pp. 1376– 1381.

[3] S. Jung and S. Pramanik, "An efficient path computation model for hierarchically structured topographical road maps," IEEE Trans. Knowl. Data Eng., vol. 14, no. 5, pp. 1029–1046, Sep. 2002.

[4] E. W. Dijkstra, "A note on two problems in connexion with graphs," Num. Math., vol. 1, no. 1, pp. 269–271, 1959.

[5] U. Zwick, "Exact and approximate distances in graphs – a survey," in Proc. 9th Annu. Eur. Symp.Algorithms, 2001, vol. 2161, pp. 33–48.

[6] A. V. Goldberg and C.Silverstein, "Implementations of Dijkstra's algorithm based on multi-level buckets," Network Optimization, vol. 450, pp. 292–327, 1997.

[7] P. Hart, N. Nilsson, and B. Raphael, "A formal basis for the heuristic determination of minimum cost paths," IEEE Trans. Syst. Sci. Cybern., vol. SSC-4, no. 2, pp. 100–107, Jul. 1968.

[8] A. V. Goldberg and C. Harrelson, "Computing the shortest path: A search meets graph theory," in Proc. ACM Symp. Discr. Algorithms, 2005, pp. 156–165.

[9] R. Gutman, "Reach-based routing: A new approach to shortest path algorithms optimized for road networks," in Proc. Workshop Algorithm Eng. Experiments, 2004, pp. 100–111.

[10] A. V. Goldberg, H. Kaplan, and R. F. Werneck, "Reach for A*: Effi- cient point-to-point shortest path algorithms," in Proc. Workshop Algorithm Eng. Experiments, 2006, pp. 129–143.

[11] S. Jung and S. Pramanik, "An efficient path computation model for hierarchically structured topographical road maps," IEEE Trans. Knowl. Data Eng., vol. 14, no. 5, pp. 1029–1046, Sep. 2002.

[12] R. Goldman, N. Shivakumar, S.Venkatasubramanian, and H. Garcia-Molina, "Proximity search in aatabases," in Proc. Int. Conf. Very Large Data Bases, 1998, pp. 26–37.

[13] N. Jing, Y.-W. Huang, and E. A. Rundensteiner,"Hierarchical optimization of optimal path finding for transportation applications," in Proc. ACM Conf. Inf. Knowl. Manage., 1996, pp. 261–268. [

[14] N. Jing, Y. wu Huang, and E. A. Rundensteiner,"Hierarchical encoded path views for path query processing: An optimal model and its performance evaluation," IEEE Trans. Knowl. Data Eng., vol. 10, no. 3, pp. 409–432, May/Jun. 1998.

[15] U. Demiryurek, F. Banaei-Kashani, C. Shahabi, and A. Ranganathan, "Online computation of fastest path in time-dependent spatial networks," in Proc. 12th Int. Conf. Adv. Spatial Temporal Databases, 2011, pp. 92–111.