International Journal of Computer Science Engineering & Technology
APPROVED BY
NATIONAL SCIENCE LIBRARY (NSL)
NATIONAL INSTITUTE OF SCIENCE COMMUNICATION AND INFORMATION RESOURCES (NISCAIR)
COUNCIL OF SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR)- NEW DELHI INDIA .
ISSN :2455-9091

A SECURITY LEVEL INTEGRATION OF IOT AND CLOUD SERVICES

[1] S. Lakshmi Priya, [2] Dr. G. Dalin
[1] Assistant professor, [2] Associate professor,
[1, 2] Hindusthan college of arts and science, Coimbatore.

ABSTRACT – The Internet of Things (IoT) provides a new paradigm for the development of heterogeneous and distributed systems, and it has increasingly become a ubiquitous computing service platform. However, due to the lack of sufficient computing and storage resources dedicated to the processing and storage of huge volumes of IoT data, it tends to adopt a cloud-based architecture to address the issues of resource constraints. Hence, a series of challenging security and trust concerns have arisen in the cloud-based IoT context. In this phase explores a new novel trust assessment framework for the security and reputation of cloud services is proposed. This framework enables the trust evaluation of cloud services in order to ensure the security of the cloud-based IoT context via integrating security-based and reputation-based trust assessment methods also proposes the STRAFbased IoT service access control.

Keywords – [Internet of Things, Cloud Services,Data Integration,ZigBee, Wireless Sensor Networks.]

1. INTRODUCTION

The 'Thing' in IoT can be any device with any kind of built-in-sensors with the ability to collect and transfer data over a network without manual intervention. The embedded technology in the object helps them to interact with internal states and the external environment, which in turn helps in decisions making process. In a nutshell, IoT is a concept that connects all the devices to the internet and let them communicate with each other over the internet. IoT is a giant network of connected devices – all of which gather and share data about how they are used and the environments in which they are operated. By doing so, each of your devices will be learning from the experience of other devices, as humans do. IoT is trying to expand the interdependence in human- i.e. interact, contribute and collaborate to things. A developer submits the application with a document containing the standards, logic, errors & exceptions handled by the tester. Again, if there are any issues Tester communicates it back to the Developer. It takes multiple iterations & in this manner a smart application is created.

Figure 1.Internet of Things

1.1 IOT ACROSS VARIOUS DOMAINS

1.1.1. Energy Applications: The energy rates have risen to a great instinct. Individuals and organizations, both are searching ways to reduce and control the consumption. IoT provides a way to not only

monitor the energy usage at the appliance-level but also at the house-level, grid level or could be at the distribution level. Smart Meters & Smart Grid are used to monitor energy consumption. It also detects threats to the system performance and stability, which protect appliances from downtime and damage.

1.1.2. Healthcare Application: Smart watches and fitness devices have changed the frequency of health monitoring. People can monitor their own health at regular intervals. Not only this, now if a patient is coming to the hospital by ambulance, by the time he or she reaches the hospital his health report is diagnosed by doctors and the hospital quickly starts the treatment. The data gathered from multiple healthcare applications are now collected and used to analyses different disease and find its cure.

1.1.3. Education: IoT provides education aids which helps in fulfilling the gaps in the education industry. It not only improves the quality of education but also optimizes the cost and improves the management by taking into consideration student's response and performance.

1.1.4. Government: Governments are trying to build smart cities using IoT solutions. IoT enhances armed force systems and services. It provides better security across the borders through inexpensive & high-performance devices. IoT helps government agencies to monitor data in real-time and improve their services like healthcare, transportation, education etc.

1.1.5. Air and Water Pollution: Through various sensors, we can detect the pollution in the air and water by frequent sampling. This helps in preventing substantial contamination and related disasters. IoT allows operations to minimize the human intervention in farming analysis and monitoring. Systems automatically detect changes in crops, soil, environment, and more.

1.2 IOT Data Integration in the Cloud

1.2.1 Internet of Things Architecture: IoT architecture can be represented with four categories of interconnected systems such as things, gateways, network and cloud Things: Today large amounts of things are found in industrial and commercial settings, it is also in users mobile and home. Already, cars, device sensors, and mobile phones are accessing the Internet through broadband wireless networks. IoT technology solution requires intelligent things capable of filtering and managing data locally and connecting to gateways easily. Gateways: The majority of existing things are not capable to connect to the internet to share data with the cloud. Because of their design. To solve this issue, gateway act as intermediate between internet and things.

1.2.2 Network Infrastructure: Internet is a complex system of interconnected IP networks that links billions of computers together. Network infrastructure comprises gateways, routers, repeaters, switches and other devices that controls the data traffic and connect with cable and telecom networks operated by different service providers.

1.3 Cloud Service Architecture: Cloud-Based Internet of Things Platform

What makes the Cloud-based Internet of Things different than conventional Internet of Things is basically the ability to develop, deploy, run, and manage Things applications online via the Cloud. Fig. 2 illustrates the main features of the Cloud-based IoT platform (i.e. CloudThings architecture) and their interaction with the three Cloud computing models of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), also specifies our technical solutions to networking Things, interacting Things, and integrating Things with the Cloud.

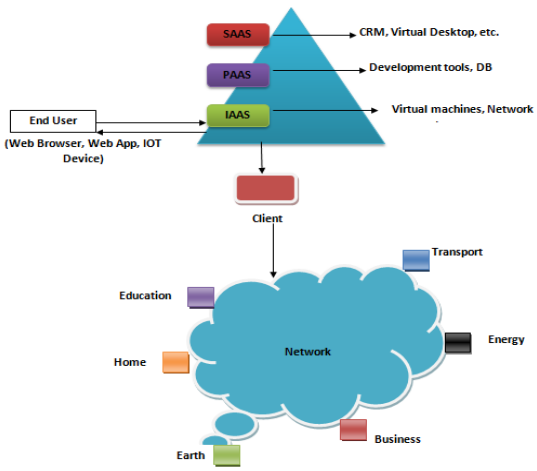

Figure 2.CloudThings architecture: the Cloud-based IoT platform

CloudThings architecture is an online platform that allows system integrators and solution providers to leverage a complete Things application infrastructure for developing, deploying, operating, and composing Things applications and services that consist of three major modules:

- The CloudThings service platform for Things is a set of Cloud services (IaaS), allowing users to run any applications on Cloud hardware. The Cloud Things service platform for Things dramatically simplifies the application development, eliminates need for infrastructure development, shortens time to market, and reduces Things management and maintenance costs.
- The CloudThings Developer Suite for Things is a set of Cloud service tools (PaaS) for Things application development. These tools include open Web service application programming interfaces (APIs), which provide complete development and deployment capabilities to Things developers.
- The CloudThings Operating Portal for Things is a set of Cloud services (SaaS) that support deployment and handle or support specialized processing services including service subscription management, community coordination, Things connection, Things discovery, data intelligence, and Things composition.

1.4 ZigBee communication

ZigBee modules are embedded solutions providing wireless end-point connectivity to devices. These modules use the IEEE 802.15.4 networking protocol for fast point-to multipoint or peer-to-peer networking. The ZigBee/ZigBee-PRO OEM RF Modules interface to a host device through a logic-level asynchronous serial port. Through its serial port, the module can communicate with any logic and voltage compatible UART; or through a level translator to any serial device (For example: Through a Max-Stream proprietary RS-232 or USB interface board). Devices that have a UART interface can connect directly to the pins of the RF module.

1.5 Wireless Sensor Network

Another key component in IoT environments is represented by sensor networks. For example, they can cooperate with RFID systems to better track the status of things, getting information about position, movement, temperature, etc. Sensor networks are typically composed of a potentially high number of sensing nodes, communicating in a wireless multi-hop fashion. Special nodes (sinks) are usually employed to gather results. Wireless sensor networks (WSNs) may provide various useful data and are being utilized in several areas like healthcare, government and environmental services (natural disaster relief), defense (military target tracking and surveillance), hazardous environment exploration, seismic sensing, etc.

	IOT	Cloud
Displacement	Pervasive	Centralized
Reachability	Limited	Ubiquitous
Components	Real world things	Virtual resources
Computational capabilities	Limited	Virtually unlimited
Storage	Limited or none	Virtually unlimited
Role of the internet	Point of convergence	Means for delivering services
Big data	Source	Means to manage

Table 1.Aspects of IOT and Cloud

2. TECHNIQUES USED IN INTEGRATION OF CLOUD SERVICES

2.1RFID

In IoT scenario, a key role is played by Radio-Frequency Identification (RFID) systems, composed of one or more readers and several tags. These technologies help in automatic identification of anything they are attached to, and allow objects to be assigned unique digital identities, to be integrated into a network, and to be associated with digital information and services. In a typical usage scenario, readers trigger the tag transmission by generating an appropriate signal, querying for possible presence of objects uniquely identified by tags. RFID tags are usually passive (they do not need on-board

power supply), but there are also tags powered from batteries.

2.2 FAHP research methodology

IoT in the healthcare has been studied and FAHP research methodology is used to rank the benefits of using IoT in healthcare. The sub categories like Quality of Life, Environmental protection and Economic prosperity were considered and weights were given from the survey data collected. On each of the criteria used it showed the priorities so that the policy makers can focus on the technologies to improve them to better serve in the area of healthcare.

3. PROPOSED SYSTEM

In this section, the STRAF, a novel trust assessment framework for cloud service based on security and reputation, is proposed. This framework is an extension from our previous work and can be divided into three main components, encompassing and detailed methods are shown in Figure 3.

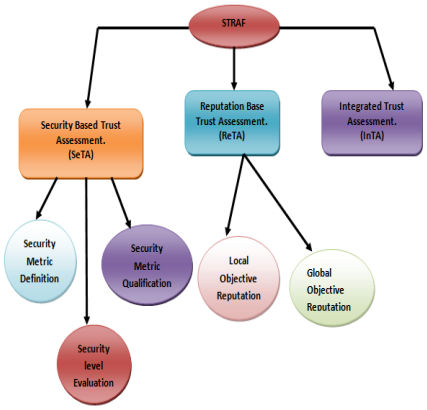

Figure 3.Hierarchy Diagram for STRAF

1. Security-based trust assessment (SeTA),
2. Reputation-base trust assessment (ReTA) and
3. Integrated trust assessment (InTA).

In addition, we further analyze the availability and feasibility of SeTA and ReTA. The STRAF includes the following components.

3.1 Security-Based Trust Assessment: The SeTA, a security-based trust assessment method, is proposed and detailed in this section. The SeTA comprises three main procedures, including

- Security metrics definition,
- Security metrics quantification, and
- Security level evaluation.

For convenience, the key notations used in SeTA Specifically, the SeTA includes the following steps.

Security Metrics Definition: In this stage, the SeTA first defines security metrics and accordingly forms security control deliverable (SCD). The SCD contains n multifaceted and cloud-specific security metrics which represent various security requirements of CSCs. Then, the SCD is provided to the m candidate CSPs for fulfillment. These security metrics in SCD are supposed to be ensured by CSPs implementing specific security controls or security mechanisms. Finally, The CSPs self-evaluates its security capability according to security metrics and provide their conformity with security metrics.

Security Metrics Quantification: The second round is to quantify the security metrics of each candidate CSP included in SCDs for convenient comparison of their security capabilities. The quantification approach depends on different types of the security metrics. In this step, we employ the quantification approach propose. The quantitative SCDs are used as input dataset Qm×n of security level evaluation process.

$$\mathbf{R_{m\times n}} = \left(\frac{Q_{ij}}{\sqrt{\sum_{i=1}^{m} Q_{ij}^2}}\right) m \times n \qquad (1)$$

$$A^+ = \{\min(r_{ij}) \mid j \in j^- \text{ or } \max(r_{ij}) \mid j \in j^+\} \quad (2)$$

$$A^- = \{\max(r_{ij}) \mid j \in j^- \text{ or } \min(r_{ij}) \mid j \in j^+\} \quad (3)$$

where, i = 1, 2, · · · , m, j = 1, 2, · · · , n, rij∈ R, J + represents the security metrics having a positive impact and J − represents the security metrics having a negative impact. After that, separation measures D can be calculated by Equations (4) and (5), which represent the geometric distance from each CSP, to ideal solutions A. It also includes positive D+ and negative D−.

$$D_i^+ = \sqrt{\sum_{j=1}^{n}(r_{ij} - r_j^-)^2} \qquad (4)$$

$$D_i^- = \sqrt{\sum_{j=1}^{n}(r_{ij} - r_j^-)^2} \qquad (5)$$

Where i = 1, 2, · · ·, m, D + i and D − i denote the separation measure from each CSP to positive and negative ideal solutions, respectively.

Security Level Evaluation: For the given quantitative SCDs Qm×n, SeTA employs the method based on technique for order preference by similarity to ideal solution (TOPSIS) to evaluate the security level of each candidate CSP and compare their security level in accordance to evaluation results.

Data Collection and Preprocessing: Define and select n security metrics according to the common security issue of cloud service and form the security metric template. m candidate CSPs fill out the SMT and submit it as security control deliverables (SCDs). Integrate and normalize the SCDs as a dataset K.

Security Controls Deliverables Quantification: In terms of CSP, the contents of dataset K (e.g., security metrics) are quantified as dataset Q according to the category of security metrics.

Security Level Evaluation: Construct the normalized decision matrix R with the quantitative SCDs Q by TOPSIS method. Determine the positive (A+) and negative (A−) ideal solutions for each security metric. Calculate the separation measures (D+and D−) in accordance with ideal solutions. Calculate the relative closeness (C) for each CSP.

Algorithm 1:Security Level Evaluation
Input: set of SCD Q, size of the set m × n
Step 1: procedure Security Level Evaluation (Q, m, n)
Step 2: Create arrays C1×m, A+ 1×n , A− 1×n , D+ 1×m,
Step 3: D − 1×m ← ∅; 4: Create matrix Rm×n ← ∅;
Step 5: R ← MATRIXNORMALIZATION (Q, m, n);
Step 6: A + 1×n, A− 1×n ← IDEALSOLUTIONS (R);
Step 7: D + 1×m, D− 1×m ← SEPARATIONMEASURES(R, A + 1×n, A− 1×n);
Step 8: C ← RELATIVECLOSENESS D + j, D− j;
Step 9: Sort(C);
Step 10: return C;
Step 11: end procedure;

3.2 Reputation-base trust assessment (ReTA)

In this process, the ReTA continuously evaluates the reputation of cloud services within several fixed-sized consecutive time windows. In each time window, the local objective reputation (LOR) is evaluated in accordance with the feedback ratings provided by CSCs. The global objective reputation (GOR), representing the holistic reputation level of all services provided by a CSP, will be obtained by aggregating the time-based weighted LOR. After that, the ReTA quantifies the reputation (i.e., GOR) of each CSP and submits it to the InTA for the integrated trust assessmentspecifically; the ReTA includes three stages as follows.

i. Local Objective Reputation

In this stage, we assume that CSCs are willing to give feedback ratings to a service that he/she has invoked, and these ratings can be collected for service reputation evaluation purpose. Since LOR is evaluated by the feedback ratings on a specific service provided by CSCs within a fixed time of period, LOR can be considered as a time window-based reputation metric for cloud service. LOR is generated in a time window when interactions have been taken place between CSCs and services.

Definition 1: Let Ω = {S1, S2, · · · ,Sm} denote m cloud services; Let Ψ = {C1, C2, · · · , Cn} denote n CSCs. Let Fij (Δtk) denotes the feedback rating of CSC Cj on cloud service Si within the time window Δtk. Let LSi (Δtk) denote the LOR of cloud service Si (Si ∈ Ω) within the k th time window Δtk. We define the LSi (Δtk) as follows,

$$L_{s_i}(\Delta t_k) = \sum_{j=1}^{n} (F_{ij}(\Delta t_k) \times \gamma_{r_j}^{(\Delta t_k)} \times \lambda_{r_j}^{(\Delta t_k)} \quad (6)$$

Where γ Δtk j and λ Δtk j respectively represent the credibility of CSC Cj and the certainty of its feedback ratings within the k th time window Δtk, which will be detailed later. The dimensions included in a feedback rating Fij (Δtk) depend on the type of feedback rating from the CSCs. For instance, if there are κ resources or attributes of a cloud service Si that CSCs focus on, Fij (Δtk) represents the feedback rating offered by CSC on the QoS of a cloud service

attribute or the holistic cloud service within the Δtk time window,

ii. Global Objective Reputation

In the previous two stages, the LORs, representing the reputation level of each cloud service in each time window, have been obtained. In this stage, the global objective reputation (GOR) which denotes the reputation level of each cloud service within an evaluation time period can be obtained by aggregating the LOR of each cloud service with time-based weights.

Definition 2: For a given consecutive time window z, let Y = {υ1, υ2, · · · ,υz} denote a time-based weight assigned to the LOR of a service Si within different time windows LSi (Δtk) (k ∈ [1, z]). Let GSi (Δtz) denote the GOR of service Si within current time window Δtz; The GOR of service Si is defined as follows.

$$G_{s_i}(\Delta t_z) = \sum_{R=r}^{z}\left(L_{s_i}(\Delta t_k) \times v_k\right) \quad (7)$$

Algorithm 3: Global Objective Reputation

Input: time windows z, feedback ratings dataset Θ of CSCs, size of dataset |Θ|
Step 1: procedure GOR EVALUATION (Θ, |Θ|, z)
Step 2:Ssize ← 0;
Step 3:Ssize ← GETSERVICESNUMBER (Θ, |Θ|);
Step 4: Create arrays SidSsize ,LSsize×z, Yz, GSsize ← ∅;
Step 5: SID ← GETSERVICESID (Θ, |Θ|);
Step 6: for i = 0 to z do
Step 7: Y[i] ← TIMEWEIGHTSASSIGNMENT (Δti);
Step 8: for j = 0 to S size do
Step 9: L[j][i] ← LOCALOBJECTIVEREPUTATION(
Step 10: Θ, |Θ|, Δti, Sid[j]);
Step 11: end for
Step 12: end for
Step 13: for j = 0 to Ssize do
Step 14: G[j] ← L[j] × YT;
Step 15: end for
Step 16: Normalize G into a unified range [0, 1];
Step 17: return G;
Step 18: end procedure;

3.3 Integrated Trust Assessment

After the processes of SeTA and ReTA, the security level and reputation level of a cloud service can be obtained. Then, in the integrated trust assessment (InTA) process, the trust level of targeted cloud services can be obtained by integrating the security level and reputation level based on the objective weight assignment approach.Inspired by this scenario, we employ objective weight assignment approach based on the actual situation to determine the relative importance weights of the security level and the reputation level obtained respectively from SeTA and ReTA. In other words, the relative importance weight of security level is determined by the ratio of its elements (i.e., security metrics) to the total number of elements involved in InTA. Similarly, the relative importance weight of reputation level is determined by the number of its elements (i.e., resources or attributes) involved in InTA. The Phase introduces a parameter ϕ to adjust the trade-off between SeTA and ReTA. Therefore, the relative importance weights of SeTA and ReTA can be determined by ϕ.

Definition 3: Suppose that Si is a targeted cloud service to be evaluated, M = {m1, m2, · · · , mu} are its security metrics, and A = {a1, a2, · · · , av} are its resources or attributes; Let U and V denote respectively the number of security metrics and attributes; Let α denotes the relative importance weight of SeTA. Here define the as follows.

$$\alpha = \frac{U \times \phi}{U \times \phi + V \times (1 - \phi)} \quad (8)$$

Where, ϕ ∈ [0, 1] is an adjustable positive constant, which can be tuned accordingly.

Definition 6: Suppose that SLi and RLi denote the security level and reputation level of cloud service Si; Let TSi denotes the trust level of cloud service Si; We define the TSi as follows.

$$TSi = \alpha \times SLi + (1 - \alpha) \times RLi \ (17) \quad (9)$$

This will lead to an overweighting of relative importance assigned to security level in InTA. Hence, to address this issue, the parameter ϕ is used as a regulatory factor to

leverage the trade-off between SeTA and ReTA.

The experiments are conducted by using MATLAB R2017b and are performed on a DELL desktop computer with the following configuration: an Intel Core i5 2.7 GHz CPU, 8 GB RAM, and the Windows 10 operating system. There is currently no integrated and available dataset fit for the validation of the STRAF (the assessment framework), namely, that are available for both SeTA and ReTA. Therefore, we use a synthesized dataset that contains some security metrics and a real-world web service dataset to validate the methods of SeTA and ReTA, respectively.

CONCLUSION

In this paper, propose a novel trust assessment framework for cloud services (named STRAF) that combines its security and reputation characters. This framework has the ability to enhance the security of the cloud-based IoT context through trustworthy cloud services. In addition, for the improvement of the accuracy and reliability of the feedback rating-based reputation assessment model, we present a reputation-based trust assessment method (namely, ReTA). Furthermore, for the sake of the potent combination of SeTA and ReTA, an integrated trust assessment method (namely, InTA) is proposed to assess the overall trustworthiness of cloud services. Simulation-based experiments validated the performance and availability of our proposed methods.

REFERENCE

[1]. AlessioBotta, Walter de Donato, Valerio Persico, Antonio Pescap, “Integration of Cloud Computing and Internet of Things: a Survey”, http://dx.doi.org/10.1016/j.future.2015.09.021 Reference: FUTURE 2851,2015.

[2]. Ismail Chahid, AbderrahimMarzouk, “A Secure IoT Data Integration in Cloud Storage Systems using ABAC Access Control Policy”, [Vol-4, Issue-8, Aug- 2017] https://dx.doi.org/10.22161/ijaers.4.8.6 ISSN: 2349-6495(P) | 2456-1908(O).

[3]. H. Manjunath, Vasangouda, Mahantesh C., PavankumarM.,”Internet Of Things (Iot) And Cloud Computing For Agriculture”,2016.

[4]. Arun K Mani, Shreevani D, Samra said, M.Gokilavani, Unnikrishnan K N, “A REVIEW: IOT AND CLOUD COMPUTING FOR FUTURE INTERNET”, p-ISSN: 2395-0072,2019.

[5]. Jiehan Zhou, TeemuLeppänen, ErkkiHarjula, Chen Yu, Hai Jin, Laurence Tianruo Yang, “CloudThings: a Common Architecture for Integrating the Internet of Things with Cloud Computing”, 2013 IEEE.

[6]. Mohammad Riyaz Belgaum, SafeeullahSoomro , ZainabAlansari, Muhammad Alam, Shahrulniza Musa, MazlihamMohdSu’ud, “Challenges: Bridge between Cloud and IoT”, 2016.

[7]. XIANG LI , QIXU WANG , XIAO LAN , XINGSHU CHEN , NING ZHANG , (Member, IEEE), and DAJIANG CHEN4 ,” Enhancing Cloud-Based IoT Security through Trustworthy Cloud Service: An Integration of Security and Reputation Approach”, Digital Object Identifier 10.1109/ACCESS.2017.

[8]. Khanista Namee1st, NuttapatPanong, JantimaPolpinij, “Integration of IoT, Edge Computing and Cloud Computing for Monitoring and Controlling Automated External Defibrillator Cabinets in Emergency Medical Service”, 2015.

[9]. JeongjuBae, Chorwon Kim, JongWonKim , “Automated Deployment of SmartX IoT-Cloud Services based on Continuous Integration”,2016.

[10]. Botta, Alessio, et al. "Integration of cloud computing and internet of things: a survey." In Proc. Future Generation Computer Systems, 56, 684- 700, 2016.

[11]. Lai, Sen-Tarng, and Fang-YieLeu. "Applying Continuous Integration for Reducing Web Applications Development Risks." In Proc. 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), 2015.

[12]. Seth, Nikita, and Rishi Khare. "ACI (automated Continuous Integration) using Jenkins: Key for successful embedded Software development." In Proc. 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), 2015.

[13]. Sanjiv M. Narayan,Paul J. Wang,James P. Daubert , “New Concepts in Sudden Cardiac Arrest to Address an Intractable Epidemic JACC State-of-the-Art Review,” Journal of the American College of Cardiology, Publisher: Elsevier, 2019.
[14]. Nadine Levick, “iRescU - Data for Social Good Saving Lives Bridging the Gaps in Sudden Cardiac Arrest Survival,” EMS Safety Foundation, 2016.
[15]. Mandler, B., Antonelli, F., Kleinfeld, R., Pedrinaci, C., Carrera, D., Gugliotta, A., &Villares, C. V. (2013, March). COMPOSE--A Journey from the Internet of Things to the Internet of Services. In Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on (pp. 1217-1222). IEEE.