International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 3, Issue 10 (October '2017)

WEB INFORMATION SECURITY WITH CLIENT AND CLOUD SERVER USING IOT TECHNIQUES

R.Vetriselvan,
M.Phil., Research Scholar,
Department Of Computer Science,
Srimad Andavan College of Arts and Science,
Trichy,Tamilnadu,India.

Dr. P.Srivaramangai,
Professor,
Department Of Computer Science,
Maruthupandiyar College of Arts and Science,
Thanjavur,Tamilnadu,India.

Abstract: Security and privacy issues have developed critically important with the fast expansion of multi-agent systems. Most network submissions such as pervasive computing, grid computing and P2P networks can be viewed as multi-agent systems which are open, anonymous and dynamic in nature. Such characteristics of multi-agent systems introduce vulnerabilities and threats to providing secured announcement. Industrial systems always prefer to reduce their operational expenses. To support such reductions, they need solutions that are capable of providing stability, fault tolerance, and flexibility. One such solution for industrial systems is cyber physical system (CPS) integration with the Internet of Things (IoT) utilizing cloud computing services. These CPSs can be well-thought-out as smart industrial systems, with their most prevalent applications in smart transportation, smart grids, smart medical and eHealthcare systems, and many more. These manufacturing CPSs mostly utilize supervisory control and data acquisition (SCADA) systems to control and monitor their critical infrastructure (CI). For example, WebSCADA is asubmission used for smart medical technologies, making improved patient monitoring and more timely decisions possible. The concentration of the study obtainable in this paper is to highpoint the security challenges that the industrial SCADA systems face in an IoT-cloud environment. Conventional SCADA organizations are already lacking in proper security measures; however, with the integration of complex new constructions for the future Internet based on the concepts of IoT, cloud computing, mobile wireless sensor networks, and so on, there are large issues at stakes in the security and deployment of these classical systems. Therefore, the incorporation of these future Internet perceptions needs more research effort.

Keywords: Cyber Physical System, Industrial Control System, Internet of Things (IoT), Supervisory Control and Data Acquisition System, SOA.

I. INTRODUCTION

Service-oriented Architecture (SOA) has become a pouring force for Web applications development. Service-oriented Computing (SOC) is a computing pattern that is driven by SOA. SOC uses services as the basic constructs to support rapid, low-cost, and easy composition of distributed applications even in heterogeneous surroundings. In SOA, a service is defined by a Web interface that supports interpretable operations between different software applications using a standard messaging protocol.

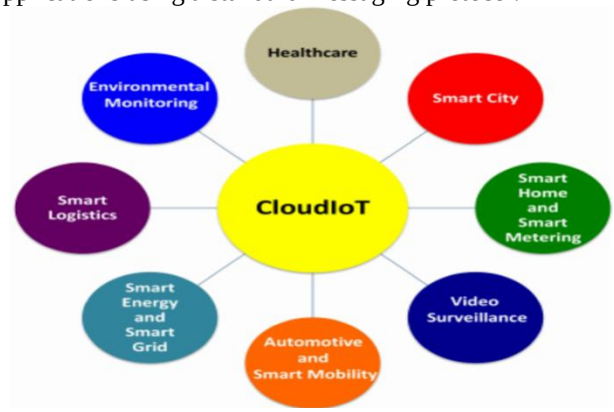

Figure 1: Cloud and IoT Application Scenario

Web services are a widespread implementation of SOA. A Web service is described by means of the Web Services Description Language (WSDL), and that description is published in a public Universal Description Discovery and Integration (UUDI) registry. XML is used to paradigm the basic blocks of Web service communication by means of some form of XML messaging, such as Simple Object Access Protocol (SOAP) request or response or XML Remote Procedure Call (XML-RPC).

Major breadwinners of Web services, such as Google, Amazon and Yahoo, have decided to publish their Web services finished their own websites instead of using public registries or brokers. This trend is forcing users to discover Web facilities using a search-engine model. Al-Masri et al. that services registered in public registries are lessening in contrast with services crawled by search engine's crawlers. The playwrights point out that more that 53% of the UDDI Business Registry (UBR) registered services are invalid, whereas 92% of Web facilities cached by search engines are valid and active. Searching for Web services using search engines, however, can result in a blockage in the discovery process, especially for non-semantic Web services because search engines do not understand the Web service functionalities delineated inthe description file. Search engines partially match the search terms entered by the user with the Web service name, location, business, or model

defined in the Web service account file to get the results back. The uses of these kinds of keywords are, by design, limited in WDSL specifications. If the examination query does not contain part of the Web service name exactly, then the service may not be recovered.

II. LITERATURE SURVEY

By implementing confidential cloud-based SCADA/HMI solution using a private cloudand the ICS with the SCADA/HMI system from Wonder ware and Rockwell Automation[8]. We extended the ICS with cloud welfares, to portion information from theSCADA/HMI and MES (Manufacturing Execution Systems) layer and used it in educationexercises. Clients can then work with data anywhere and extend their ownSCADA/HMI answer with cloud stored data from real technology process. Technologicalprocess is without risks and the joining to the field devices is limited.Also, we consider the option if someone unauthorized gets access to the cloud storeddata or some students try to do something unauthorized.To design a cost-effective explanation for a small company, and aexplanation with closedtechnological, layers we chose to use a private cloud. Another reason was the situation when providers do somechanges in their security or service functionality.

TheSCADA/HMI and another layer of the ICS might be delicate to such changes, whichmight endanger processes in the manufacturing company (for example slowing down queryexecution). We used our own private cloud solution and with OpenVPN (Open VirtualPrivate Net) admission (for external customers and suppliers) to have better security, bemore flexible in customization and see all needed sources for realization.In our solution for the SCADA/HMI and the cloud application, we firstly createda storage place. We implemented a NAS (Network Attached Storage) through a CIFS(Common Internet File System) [9]. A NAS is a storing device for VMware virtualmachines. This implementation enables HA (High Availability) and gives individualityto the SCADA/HMI application from the hardware application on the serverside. If the physical server fails, another server will be used to continue processing data.

Data is not bound to the attendant but to the data storage. In our solution, we implementedan outside SCADA/HMI cloud solution. This answer can be set in a small industrialcompany which needs to share large amount of data to their customers, suppliers orinternal workers. The solution will be used to share data from the SCADA/HMI layer. Data storage systems should meet selected requirements (high availability, dependabilityand others) [2]. These requirements might be in conflict. For example, availability,scalability and data consistency might be in conflict [1, 2]. In our solution, we usedMySQL Cluster [11], where we gave more importance to data availability [10].Not only storage data is important, but also the infrastructure for accessing it. Becausewe chose the implementation of a private cloud in our experiment, we applieda service oriented architecture (SOA) in our architecture with a service thatretrieves data from the communication server. The communication server interconnectswith the technological layer of our ICS. The service is also used to saving data tothe mist storage and its retrieval. The service communicates with HMI customers.

III. METHODOLOGY

The following general security considerations apply to SCADA systems:

1) Policy Management: Cyber security is considered a danger because if an interloper somehow gains access to a SCADA system then the intruder most probably also gains control over everything within the organization. The threats increase enormously when these organizations are connected to the Internet. For example, protecting SCADA systems against Internet connectivity was not even considered a possible vulnerability when power systems were first developed. Because people often have little consciousness of the methods for securing CIs, cyberattacks are snowballing. To assess power system vulnerabilities, an attack tree model was used by Watts. The author argues that good keyword policies make the scheme access points strong and make it difficult for an intruder to guess a password to access the systems. A disadvantage of this methodology is that attack trees do not capture the penetration sequence of attack leaves.

Cagalaban et al. present a responsibility detection algorithm to find the susceptibilities in SCADA system software. The authors of used a test-bed architecture and the Modbus protocol. The purpose of an attacker can be easily identified by this methodology. The consequences reveal that SCADA systems software strength increases when these systems follow proper rules for substantiation and approval.

2) Data Integrity: To mitigate Denial of Service (DoS) attacks, Davis et al. accepted a test-bed architecture using RINSE, which also assesses vulnerabilities faced by power systems. Three attack scenarios are considered. In the first situation, there is no attack and systems perform normally; in the second scenario, the DoS attack is presented; and the last scenario applies filters such that the effects of a DoS attack can be measured. A disadvantage of this methodology is that it focuses only on the software level; hence, hardware is not taken into consideration. Giani et al. presented a test-bed architecture in which system availability and integrity are compromised by introducing multiple attacks. The major goalmouth of this study was to measure the impact that such attacks have on SCADA systems. Davis et al. proposed a few models to investigate attacks, determine their effects, and identify mitigation strategies. Obtainable a methodology that detects such attacks by monitoring and analyzing the bodily system under observation. As recommended by attack-resilient algorithms are required to make the systems able to survive deliberate attacks such as Stunned.

3) Weak Communication: Rendering to the communication links of SCADA systems can be attacked easily because they do not typically provide encryption and verification mechanisms. The American Gas Association (AGA) has played a vital role in securing SCADA system infrastructures and presented the concept of cryptography within these systems' communication. Protected SCADA (sSCADA), a plugin device, is presented in as Part 1 of the

AGA's cryptographic standard, with two vulnerabilities that lead to man-in-the-middle and replay attacks speech these vulnerabilities, the authors propose four channels of communication, each fulfilling different security services. The job of an attacker is made easy by the use of a weak protocol. The communication protocols used in SCADA systems are responsible for communicating messages over the entire industry network. Many protocols are used including DNP3, PROFIBUS, Ethernet/IP, etc., but based on the system necessities a particular protocol is selected for communication. The devices that were considered as trusted were connected to the SCADA systems network long before security issues were taken into contemplation. Use of the new Internet-based knowledge established untrusted connections.

IV. EXPERIMENTAL RESULT AND DISCUSSION

In order to verify our algorithm, we conducted experiment on Intel(R) core(TM) i5 Processor 2.6 GHz, Windows 7 platform and using Java 3.0.3 simulator. The NetBeans toolkit supports demonstrating of cloud system components such as data centers, host, virtual machines, preparation and resource provisioning policies. A instrument kit is the consumption which open the possibility of evaluating the hypothesis prior to software development in an environment where one can reproduce tests We have created 5 Virtual Machines using VMconstituent and set the stuff of RAM as 512 MB for all Virtual Machines, and the MIPS as 250, 1000, 250, 500 and 250 respectively. We have created 12 tasks using Cloudlet component and set the property of Cloudlet length as 20000, 10000, 20000, 10000, 10000, 20000, 10000, 20000, 10000, 10000, 20000 and 10000 respectively. For this we considered 5 Virtual Machines with MIPS 1000, 500, 250, 250, 250 and RAM size of all Virtual Machine as 512 MB. Experiment is conducted for varying number of tasks like 100, 200, 300, 400 and 500 respectively.

Scenario 1: When there is main difference among slowest and wildest resource. Assume that Task scheduler has meta-tasks and possessions as given below.

Table 1.1, represents the volume of instructions and data in tasks T1 to T5.

Task	Instruction Volume(MI)	Data Volume(Mb)
T1	1400	68
T2	1600	67
T3	1200	45
T4	800	56
T5	1000	97

Table 1.2, represents processing speed and bandwidth of communication links of each resource.

Resource	Processing Speed (MIPS)	Bandwidth(Mbps)
R1	100	150
R2	400	50

Using data given in Table 1.1 and Table 1.2, to calculate the expected execution time of the tasks on each of the resource.

Task	Resources	
	R1	R2
T1	14	3.5
T2	16	4
T3	12	3
T4	8	2
T5	10	2.5

Table 1.3 Execution time of the tasks on each resource

Figure 2: Performance Comparison between Existing and Proposed Approaches

Rendering to the implementation results, it is found that the proposed *BFPSOTS* algorithm outperforms the standard *PSO* procedure by 18.71%, 16.45%, and 13.99% in average with respect to Makspan, resource utilization, and implementation cost respectively. In spite of the time complexity of the future*BFPSOTS* algorithm, it outperforms the standard *PSO* algorithm with respect to Makspan, implementation cost, and resource consumption.

V. CONCLUSION

The objective of this edification was to highlight some importantfacts about industrial SCADA systems with an emphasis onthreats, vulnerabilities, administration and the current practicesbeing followed. CPSs such as SCADA systems arewidely used. The objective of IoT-based SCADA systemsis to increase their flexibility, cost efficiency, optimizationcompetence, availability and scalability of such systems. Forthis purpose, industrial SCADAsystems utilize the welfares ofIoT and cloud computing. However, these benefits are accompaniedby abundantdangerous risks. Major security risks relatedto the industrial SCADA systems in the cloud may vary fromone situation to another. In such environments, the nature ofdata is such that it must be stored on server/s for backup ordistribution purposes, and these server/s are mostly

managed bya third party. This third party management means that theseservers are likely to contain large statistics of clients andtheir confidential information. The result is that the privacyof data on these cloud servers cannot be guaranteed, as thedata may or may not be communal with other clients. Therefore,such security breaches must be considered before assimilatingindustrial SCADAsystems with IoT-cloud surroundings.

Future Work:

Real-Time Data Handling: CPSs such as IoT, which are principally based on supervisingand controlling data acquisitions, need to collect and examinethe data in real time and make business decisions; thesesystems cannot afford delays. For such decision manufacture, classicalCPSs utilize local decision loops, but with the cloud andIoT, they are flattering more dependent on external services.Therefore, aspects of timely interaction need to be revisited.

Cross-Layer Collaborations : The efficiency of these systems depends on collaborationamong the complicated platforms that are responsible for deliveringservices in a service-based substructure. However, thesecomplex collaborations possess multiple requirements fromboth the business and technical worlds that are based on specific application situations. To make the CPS ecosystem flourish, people need assurance that these complex partnershipscan deliver services efficiently and effectively butproviding that declaration is not an easy task and needs moreinvestigation.

VI.REFERNCES

[1]. T. Lojka and I. Zolotová, ``Improvement of human-plant interactivity via industrial cloud-based supervisory control and data acquisition system," Advances in Production Management Systems. Innovative and Knowledge-Based Production Management in a Global-LocalWorld (IFIPAdvances in Information and Communication Technology). Berlin, Germany: Springer, 2014, pp. 8390.

[2]. C.-R. Rad, O. Hancu, I.-A. Takacs, and G. Olteanu, ``Smart monitoring of potato crop: A cyber-physical system architecture model in the eld of precision agriculture," Agricult. Agricult. Sci. Procedia, vol. 6, pp. 7379, Sep. 2015, doi: 10.1016/j.aaspro.2015.08.041.

[3]. G. Fortino, A. Guerrieri, and W. Russo, ``Agent-oriented smart objects development," in Proc. IEEE 16th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD), May 2012, pp. 907912.

[4]. W. Wei, X. Fan, H. Song, X. Fan, and J. Yang, ``Imperfect information dynamic stackelberg game based resource allocation using hidden Markov for cloud computing," IEEE Trans. Services Comput., vol. PP, no. 99, p. 1, Feb. 2016, doi: 10.1109/TSC.2016.2528246.

[5]. I. Butun, M. Erol-Kantarci, B. Kantarci, and H. Song, ``Cloud-centric multi-level authentication as a service for secure public safety devicenetworks," IEEE Commun. Mag., vol. 54, no. 4, 2016.

[6]. H. Song, Q. Du, P. Ren, W. Li, and A. Mehmood, ``Cloud computing for transportation cyber-physical systems," in Cyber-Physical Systems: A Computational Perspective, vol. 15, L. M. Patnaik, Ed. Boca Raton, FL, USA: CRC Press, 2015, pp. 351369.

[7]. Y. Sun, H. Song, A. J. Jara, and R. Bie, ``Internet of Things and big data analytics for smart and connected communities," IEEE Access, vol. 4,pp. 766773, Mar. 2016, doi: 10.1109/ACCESS.2016.2529723.

[8]. H. Abbas, M. Q. Mahmoodzadeh, F. A. Khan, and M. Pasha, ``Identifying an OpenID anti-phishing scheme for cyberspace," Secur. Commun. Netw., vol. 9, no. 6, pp. 481491, 2014.

[9]. H. Abbas, C. Magnusson, L. Yngstrom, and A. Hemani, ``Addressing dynamic issues in information security management," Inf. Manage.Comput. Secur., vol. 19, no. 1, pp. 524, 2011.

[10]. K. Saleem, A. Derhab, J. Al-Muhtadi, and B. Shahzad, ``Humanoriented design of secure machine-to-machine communication system fore-healthcare society," Comput. Human Behavior, vol. 51, pp. 977985, Oct. 2015.

[11]. H. Khattak, H. Abbas, A. Naeem, K. Saleem, and W. Iqbal, ``Security concerns of cloud-based healthcare systems: A perspective of movingfrom single-cloud to a multi-cloud infrastructure," in Proc. 17th Int. Conf. E-Health Netw., Appl. Services (HealthCom), 2015, pp. 5056.

[12]. B. M. C. Silva, J. J. P. C. Rodrigues, I. de la Torre Díez, M. López-Coronado, and K. Saleem, ``Mobile-health: A review of current state in 2015," J. Biomed. Inform., vol. 56, pp. 265272, Aug. 2015.

[13]. (2016). WebSCADA, Web SCADA, Automation Systems, Process Control, Historian, Event Alarm, SCADA Solution, accessed on Feb. 5, 2016. [Online]. Available: http://www.webscada.com/SCADA/SolMedSys.aspx

[14]. R. J. Robles and M.-K. Choi, ``Assessment of the vulnerabilities of SCADA, control systems and critical infrastructure systems," Int. J. Grid Distrib. Comput., vol. 2, no. 2, pp. 2734, 2009.

[15]. `Flame' Spyware Inltrating Iranian Computers, CNN, Atlanta, GA, USA, 2012.

[16]. J. D. Fernandez and A. E. Fernandez, ``SCADA systems: Vulnerabilities and remediation," J. Comput. Sci. Colleges Arch., vol. 20, no. 4, pp. 160168, Apr. 2005.

[17]. N. Ulltveit-Moe, H. Nergaard, L. Erdödi, T. Gjøsæter, E. Kolstad, and P. Berg. (2016). ``Secure information sharing in an industrial Internet of Things." [Online]. Available: http://arxiv.org/abs/1601.04301

[18]. M. Bere and H. Muyingi, ``Initial investigation of industrial control system (ICS) security using articial immune system (AIS)," in Proc. Int. Conf. Emerg. Trends Netw. Comput. Commun. (ETNCC), 2015, pp. 7984.