

Devices of Computer Network Security and Visualization Control System: Design and Implementation

Satar Habib Mnaath^{1*}, Ahmed Dheyaa Basha², Rozinah Jamaludin³, Irfan Naufal Umar⁴

¹Center for Instructional Technology and Multimedia (CITM), Universiti Sains Malaysia, Penang, 11800
s2s2_066@yahoo.com

ABSTRACT

Depending on the applications of analysis for the control technology in the computer visualization network security protection and security procedures, from the corners of the natural / physical environment and software of the network system and environmental security. This article offers a security system monitoring solution recognize the network using the tools of Internet (TOI), communications and other visualization technologies. Security perceptions of Control System In environments of computer network, using radio frequency identification (RFID) of TOI and integration of communication technology for the implementation of systems integration design. In the security environment of network physical, gas, temperature, humidity, and visualization technologies to do overseeing all environmental data, technology is used dynamic visualization environment security network system, and a user-defined security some impact items, used record protection for data analysis fast, and extends control of the interface I/O through the evolution of the API and the AT command, computer and network security monitoring imagine based on the Internet and GSM/GPRS is obtained. That enables the users to perform interactive visualization and control of network security an environment by E-MAIL, WEB, also PDA, mobile phone a short message and the Internet. In testing system, through the intermediate server, security data visualization and information in real time with the deflection has been achieved 3-5% that has proven the feasibility of the computers network security, Awareness system control.

Keywords: Network Security; Computer Network; Visualization Network Security; Protection System.

1 INTRODUCTION

The best solving is computer network security among the combining all types of systems, modem networking technologies, network equipment, network software, information systems and other security complementary technologies, using chain of network security protection systems and consistent format possibilities, Attacks and threats in real-time and physical harm in networking environments, perceptions computer network security is a mechanism that to control the using network system management technology computer and communication technology integration [1]. It maintains online contact with the user's administrated or achieves real-time notification network security matters for automatic communication technology for network communications complementarities. Visualization of control a specific form of expression on the status of the protection of information, communication network. Users can reply accordance with that interactive manner and to take specific security measures, in order to Privacy Policy of data, and complementarily in implementation. There are two kinds of security in network security first logic security second physical security in terms of Computer Network Security visualize System, (CNSVS)[2].

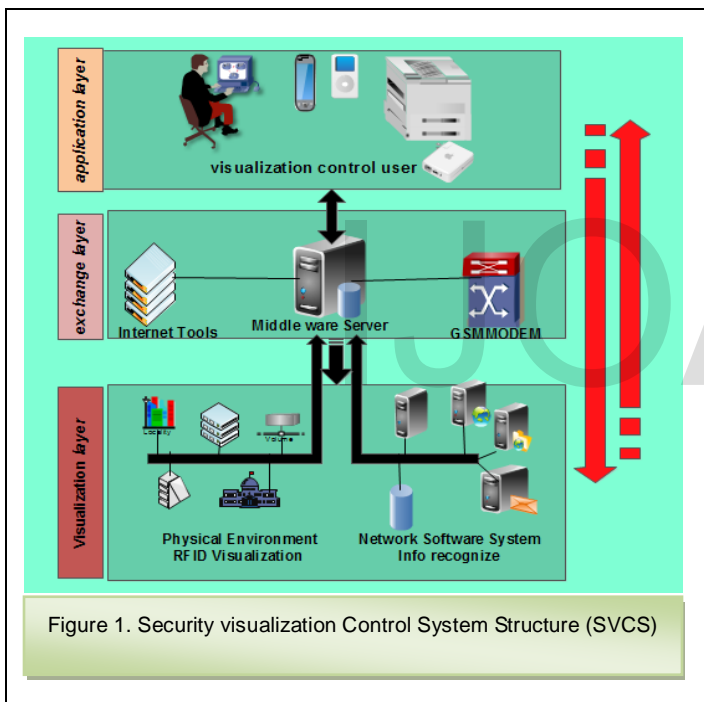
Physical protection system hardware and physical security environment are physical security, for example, such as humidity, temperature and gas in the network environment,

as well as fire prevention, Some programs, such as Ante Virus protection and other security proceedings in the environment[3]. All the security cases of OS, device, data and so on in the computer network system when it is under attack, Located under the name logic security measures. Computer network security (CNS) is a complex system engineering, which involves the environment, communications, and network as well as many of the other aspects of hardware and software technologies. Logic security includes the security issues of operating system, data, and device and so on in the computer network system when being under attack. Computer network security is a complex engineering system, which includes the environment, communications, and network as well many of the other aspects of hardware and software technologies.

Depending on an information sensing angle, the visualization technology providing ,(TOI) into physical environments, uses (RFID) to sense the humidity, gas, temperature, and other physical changes in the CNS, and through (TOI) of communications and Internet performs information exchange and aware intelligent security control (ISC)[4]. In the software environment of network system, security perception strategy is formed by assault difference or attack, protection log, programs and so on, and across (TOI) of communications and Internet performs Information exchange and aware (ISC) also too.

2 STRUCTURE OF SECURITY VISUALIZATION CONTROL SYSTEM (SOSVCS)

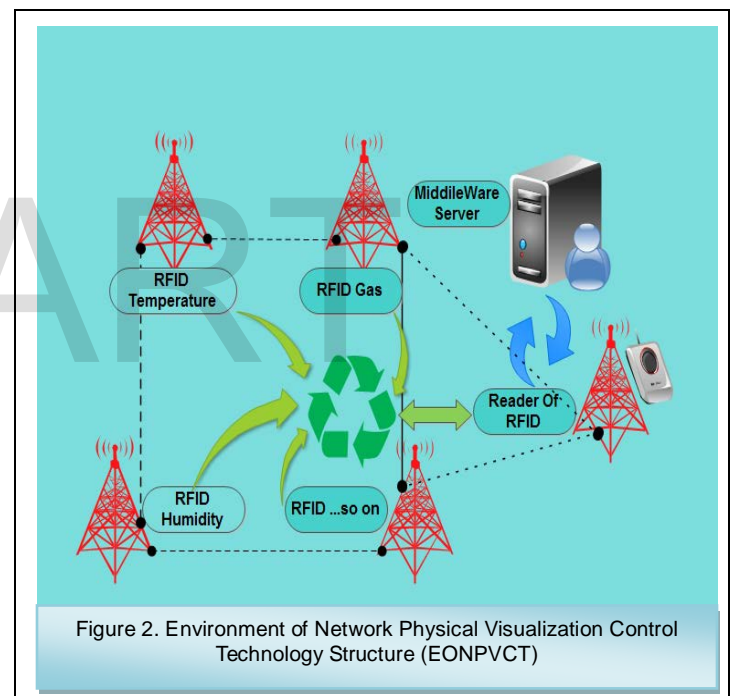
The architecture of hardware terminal sensing system settled by RFID sensing technology based on (TOI), mean Physical environment. a security control system consisting of network physical environment and network software system as well mean Computer network security is network software system security(NSSS) is to recognize the security policy of computer network software system (CNSS)[5] . Physical and software security system control share a common base to implement the movement of information via the Internet or communication devices. GSM Modem used here to accomplish information switch by short message of mobile phone, mobile voice and Internet. The system depends B/S model of 3 layers, users could use the WEB, short message to do management, exchange, analysis, command sending and other operations through all types of terminals like PDA, PC, mobile phone, and so on[6, 7]. Figure1 showed (SVCSS).



In the system there are three layers, the first one is visualization layer. It could use RFID hardware information to accomplish information visualization on network physical environment and could carry out security visualization on software systems in computer network by programs. The second one is the switch layer, it carries out information switch with system during Internet device and GSM Modem telecom communication device, the server is middleware software to perform analysis of information and communication with the application layer and the layer visualization of the system [8]. Application layer is the third layer, this layer for users, which is basically to make possible users to accomplish information control with the system during mobile device's short message, Internet, the WEB and other ways.

3 NETWORK PHYSICAL ENVIRONMENTAL SECURITY VISUALIZATION CONTROL (NPESVC)

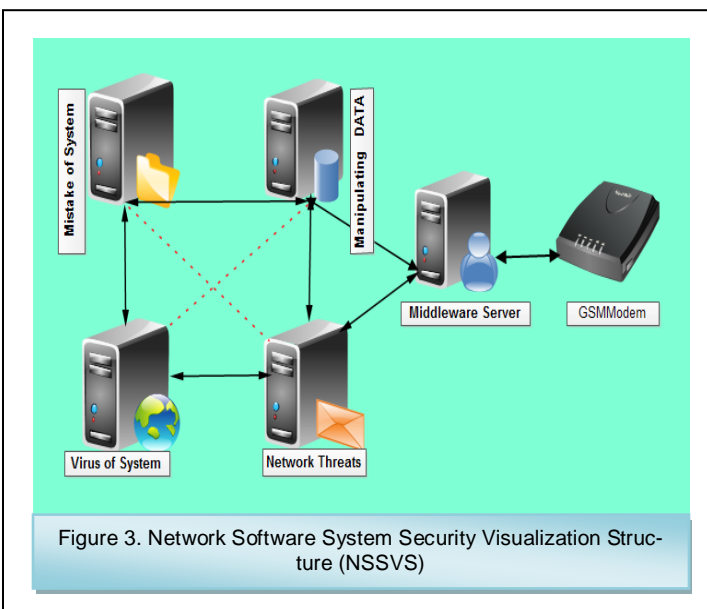
In physical environment of computer network , RFID sensors for humidity, gas, temperature , etc.... where installed in different environments via (TOI) and wireless technology transfer via WIFI, TCP/IP, or GSM/GPRS network, Transmission of sensor is occurs the sensor sends the data override system security limits detected location to RFID reader across GSM network and Internet, and transmits and pushes the information In the direction of middleware server[9].So the Middleware server (MIDS) would analyze the information and send the information to users across GSM Modem and Internet. After users receive the information, commands such as device switching on, temperature adjustment, powering off, etc.... Will be sent by users to the system via WEB, devices of phone short message and the Internet, and RFID could control the device accordingly. Figure 2 shown the situation of Network Physical Environment Security visualization Control Technology Structure.



All readers of GMS/GPRS / TCP/IP, WIFI, could adoption RFID radio signals of 2.4 --2.5 GHZ[10]. Depend on various physical environments, RFID reader resistant for the metal, water and rust could realize Long-term transmission with RFID. As well as there are three parts of RFID reader: Humidity, temperature, gas sensor of simulation, single slice and radio receiver module, and its own label by unique identifier. The parameters of the physical environment are saved in FLASH of RFID, and then sent directly to single slice to process and addresses. A Single slice plays a wide role about the command programming center and control, when the information about environment difference signals arrived, directly it intelligently converts and amplifies the signal across A/D, and then forwards the digital signal to the transceiver and intermediate server.

4 NETWORK SOFTWARE SYSTEM SECURITY VISUALIZATION CONTROL (NSSVC)

Because of the Computer networks are open system and multi-tasking, human attack, system failure, and access to information illicit important system data hexes, Crash the solid parts of the device, computer virus and many other network security threats could occur[11]. The computer network is very weak, and open the entire network technology makes the network susceptible to attacks from the communications Protocol and physical transmission line, hardware, software gaps and other aspects. Moreover too many of networks haven't any restrictions on the applications of the user. Users can browse the Internet, download and share all types of information freely and network has one aspect of freedom, but it also has across from the potential risks. The information stored in the database also opposite and facing security cases, also the user can break through illicit access to the database through the network unlawfully and must be avoided the existence of data and information conflict with connotations in the database. Actually there are a lot of network security risks, it desires and needs to establish a second layer of ISNR measures, regardless of firewall and resolve security flaws, so as to enable user's administrations to recognize of security information directly from the system and prepare for it in previously. As well as same physical system security visualization, it uses GSM Modem for Information transmission with the Internet. By the USB port or serial port, GSM connects with system(s), and recognize devices by depicting dynamic state, aware of data analysis for rapid information system security as well as the extended control for I/O ports. Figure 3 view (NSSVT) the structure.



Network software system (NSS) registers, dynamic operational status by running the system on the client side in the
Copyright © 2013 SciResPub.

scenes, and leads continue to monitor and compare to get vital information, Record protection and other information from programs work in the system security by design parameters. When the system reveals unnatural data, and carried out by Statistical analysis of the data through the control system, and shapes Curvature contrast parameters for comparison purposes, and displays the security situation in the forms of the list of parameters and real-time curve charting.

In this moment it also launches warning. The program sends a warning to the director of user e-mail alarm and other information via the Internet, or voice telephony, mobile phone SMS, Buzz and other methods via a modem to alert. , security control command could be sent to system through WEB, mobile phone SMS and other methods as well. When the administrative user receives the alarm information

5 ACHIEVING THE VISUALIZATION OF SECURITY CONTROL SYSTEM (AVOSCS)

Conceived strategy computer network security (SCNS) and control via the Internet, and email warning and other models are the only part of the Security policy, for those users who are not able to be online all the time and information visualization cannot be received in a timely manner. To complete the swap information and control comprehension in different habits, SMS of mobile phone, voice remote control understanding style depends on the GSM Modem are listed under into (SCS).

The visualization control mode based on GSM Modem depends on API programming interface and AT dictation for system programming[12]. To comprehend exchange control process with system during mobile phone and permit the system of mutual process and actual time. To test the solution, we conducted the analysis using SMS to restart the system remotely via network security control. First we are going to define device or machine code, For COM interface, baud rate, GSM Modem control and so on. As below:

```
private void Form1_Load(object sender, EventArgs e)
{
    txtQHM.Text
    GMS.GSMModemGetSnInfoNew(txtCOM.Text,
    txtBTL.Text); // GSMModem machine number
    txtCOM.Text = GMS.GSMModemGetDevice(); //
    COM interface
    txtBTL.Text = GMS.GSMModemGetBaudrate(); //
    Baud rate
    labStatus.Text = "Close service ";
}
private void Restart System()
try
{
    ConnectionOptions op new
    ConnectionOptionsO; // Specify the Settings needed to
    generate WMI connection
    op.UName = txtUser.Text; // Remote network
    system user name
    op.Password = txtPWD.Text; // Remote network
    system user password
    ManagementS cope scope = new ManagementScope("\\ \\ \\ \\")
```

```
+ txtIP.Text + " \root\ cimv2", op); //
Set operating management scope
scope.ConnectO; // The ManagementScope
connected to the system WMI range
ObjectQuery oq = new ObjectQuery("SELECT *
FROM Win32 OperatingSystem");
ManagementObjectSearcher query = new ManagementObjectSearcher(
scope, oq);
ManagementObjectCollection queryCollection
query.GetO;//Get WMI controls
foreach (ManagementObject obj in queryCollection)
{
obj.InvokeMethod("ShutDown Ir", null); // Executive
restart remote system
}
}
catch(Exception ex)
{
Process p = new Process ();
p.StartInfo.FileName = "cmd.exe";
p.StartInfo.UseShellExecute = false;
p.StartInfo.RedirectStandardInput = true;
p.StartInfo.RedirectStandardOutput = true;
p.StartInfo.RedirectStandardError = true;
p.StartInfo.CreateNoWindow = true;
p.StartO;
p.StandardInput.WriteLine(" shutdown Ir");
p.StandardInput.WriteLine("exit");
}
}
private void timer1_Tick( object sender, EventArgs e)
{
if(GMS.GSMModemInitNew(txtCOM.Text,
txtBTL.Text, null, null, false, txtPower.Text) == false) //
Link device
{
MessageBox.Show(" Failure connection! " +
GMS.GSMModemGetErrorMsg(), " Tip ", MessageBoxButtons.
OK);
return;
}
string str = GMS.GSMModemSMSReadAll(1); //
Receive text messages
if(str==null)
return;
if(str.Substring(str.IndexOf("I")+ 1, 2)
restart ")
" System
{
this. Close Windows();
}
}
private void button1_Click( object sender, EventArgs e)
{
if(button1. Text == "Open service ")
{
timer1.Enabled = true;
labStatus.Text = " Acquisition restart command ";
button1.Text = " Stop service ";
else
}
}
{
timer1.Enabled = false;
button1.Text = " Open service ";
labStatus.Text = " Close service ";
}
}
```

For other services to realize the security, it can refer to the program mentioned here for the design, in order to achieve security and oversight functions more interactive.

6 TESTING AND CONCLUSION

The model of (CNSVCS), from the point of perception about the security case as the actual control information from the physical network, environment of software system by user, and makes the whole system in case of handy and controllable status in easily. RFID in the physical environmental cognition, each sensor of RFID or tag numbers of their, own identity, and responding to control their surroundings and environments. So if RFID under observation sends security warning information, the ID number of information will collect from DB immediately by the server of middleware. Here we have for example in station 1 there are device room 10, the eighth cabinet is too hot, temperature is 75° C , also there are more information. The visualization RFID tag or label could be send information at a distance of 10-1000M, with visualization aberration of 3-5%. Data security measured through observation of the network system. Around 62ms-171ms his time for data analysis, as well the user can receive the information via mbilephone SMS with speed at (3.1~3.9) s. Response time of e-mail, data and information on the web is 562ms around. Table 1 show that.

TABLE 1. TESTING

Testing project	Practical value	Standard	Error
humidity by RFID	27	26	4%
Message control	3.4s	3.7s	<4%
temperature by RFID	55	52	3%
e-mail	530ms	570ms	<2.5%
gas by RFID	330	323	2%
SMS visualization	3.1s	3.1s	<5%

By (CNSVCS) user can understand network security status visualization in terms of controllable information; these are not mere leap from the application of computer network by (TOI) Technology, but also a surge of computer communication technology (CCT). Dynamic visualization of security and actual-time management of the network system, and enhance the security of the network to manageable level of intellectual visualization. This Service can be applied to the visualization help network infra and Internet service of Industry bear more work and network security and maintaining the security of the overall network. So this is a new mutation of the management

mode and management thinking. Development and improvement of state security network visualization technology will pump new force to the field of the network security.

REFERENCES

- [1] Z. Wang, "Design and realization of computer network security perception control system," in *Communication Software and Networks (ICCSN)*, 2011 IEEE 3rd International Conference on, 2011, pp. 163-166.
- [2] V. Gorodetski, I. Kotenko, and O. Karsaev, "Multi-agent technologies for computer network security: Attack simulation, intrusion detection and intrusion detection learning," *International Journal of Computer Systems Science & Engineering*, vol. 18, pp. 191-200, 2003.
- [3] E. K. Wang, Y. Ye, X. Xu, S. Yiu, L. Hui, and K. Chow, "Security issues and challenges for cyber physical system," in *Green Computing and Communications (GreenCom)*, 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom), 2010, pp. 733-738.
- [4] W. Ying, "Design and realization of mobile information collection module in logistic Internet Of Things Unified Information System," in *Business Management and Electronic Information (BMEI)*, 2011 International Conference on, 2011, pp. 36-39.
- [5] K. Sohrawy, D. Minoli, and T. Znati, *Wireless sensor networks: technology, protocols, and applications*: Wiley-interscience, 2007.
- [6] X. Z. Lin, "Intelligent Flexible Reform Technology of Logistic Unified Information System Based on Internet of Things," *Advanced Materials Research*, vol. 217, pp. 1343-1348, 2011.
- [7] Y. Wei, Y. Lian, and D. Feng, "A network security situational awareness model based on information fusion," *Journal of Computer Research and Development*, vol. 46, pp. 353-362, 2009.
- [8] X. Z. Lin, "Guangxi, China-ASEAN Uniform Information Joint Development of Manufacturing and Logistics Industry," *Applied Mechanics and Materials*, vol. 52, pp. 2099-2104, 2011.
- [9] R. V. Kulkarni and G. K. Venayagamoorthy, "Particle swarm optimization in wireless-sensor networks: A brief survey," *Systems, Man, and Cybernetics, Part C: Applications and Reviews*, *IEEE Transactions on*, vol. 41, pp. 262-267, 2011.
- [10] X. Lin, "Logistic geographical information detecting unified information system based on Internet of Things," in *Communication Software and Networks (ICCSN)*, 2011 IEEE 3rd International Conference on, 2011, pp. 303-307.
- [11] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *computers & security*, vol. 28, pp. 18-28, 2009.
- [12] L. M. Guerra, J. E. Fitzpatrick, and M. D. Womack, "System, method and computer program product for a dynamically configurable voice portal," ed: Google Patents, 2007.