Consumers Triggering Factory Robots Over the InternettoOptimize Purchasing Systems

Prashobh Karunakaran
University of Technology Sarawak (UTS),
SET CRISD
prashobh.karunakaran@gmail.com;

M. Shahril Osman
University of Technology Sarawak (UTS),
SET CRISD
drshahril@ucts.edu.my

***Abstract*—Demand prediction has become a big business. Google, Facebook, X etc.thrive on helping predict demand levels as well promote products. Google is doing well because of their ability to make the best demand prediction for existing products and predict future trends. The current purchasing system is causing economic waste. Today if products are not sold, they are dumped by supermarkets, wholesalers, warehouses, and factories. But if an efficient purchasing system where customers' credit card approval immediately triggers factory robots to manufacture products,itis possible to cut out the need to make demand predictions. This will lead to a purchasing system where customers deal directly with factories, which is favorable to producers as they reduce waste due to improper demand prediction and customers who will have to pay less as the middlemen are cut out; the typical manufacturing cost is only 10% of what customers pay for products.**

***Index Terms*—Demand prediction, factory robots, purchasing.**

I. INTRODUCTION

Systems are currently available, whereby as soon as a customer, somewhere in the world, credits money for a product, humans and software processthese orders and give instructions to other humans in factories to produce the product. Dell is foremost in using this strategy. It must be noted that the typical manufacturing cost is only 10% of what customers pay for the product [1].

During this author's14 years working experience at the Western Digital (WD) factory in Kuching, Malaysia up to 100,000-200,000 computer hard disk platters needed to be scrapped due to wrong prediction of demand levels[3].

The reduction of wastage all along the line from supermarkets to factories plus the lean system whereby factories deal directly with customers will result in cheaper products for everyone and especially a great reduction of waste in valuable resources as the number of products produced is exactly what customers need. There will be no need to predict demand levels. The predictive algorithms created by the likes of Google, Facebook, X, LinkedInetc. need not be applied anymore [4].

The history of marketing is that in the 1980s marketers, for example, if a new packed food product is manufactured, a market specialist was hired, and he / she would send physical survey letters to about 2000 people with a return envelope with a stamp within. Only a small percentage of the targeted people will return the filled-up survey [4].

Then came Google which as of 2024 makes almost all its parent company's revenue from advertising [5].Later the likes Facebook,WhatsApp (20 times larger than Instagram), Instagram, X, LinkedIn etc. entered the fray from which data is mined to determine consumer demand [6]. These are also advertisement companies which push products to people according to the data mined from consumers. Therefore, the low return rate of the survey letters has been replaced by Google scanning people's emails, video conferences (Google Meet). Google Home Speakers and Home Audio systems can listen to all conversations within homes. Then came Amazon, which is now the second largest retailer on earth which needs to make accurate predictions of demand levels as a very critical element in their business or else they would be purchasing products and scraping it at scrap yards when consumers do not purchase them. This would be bad for Amazon as well as thesustainability of the whole earth. Therefore, instead of paying Google etc. for this service, they came up with Alexa to determine demand levels for specific products [7].

A big portion of AI development in Alphabet Inc. (parent company of Google) and Meta (parent company of Facebook), X and LinkedIn is linked to this need to predict demand levels for specific products [8][9].

This research is to study the next step of factory to consumer link, which is to get factory robots to manufacture the product as soon as the money is credited from customers' credit cards. Thereby there is no longer a need to make predictions.

Eventually the function of the likes of Google would be to build consumer trend builders. Today the biggest obstacle to achieving such a system is security issues. If hackers can hack into factories and start making robots perform wrong tasks, production will be jeopardized. Therefore, security software must be developed or sourced from experienced anti-virus software developers, the likes of McAfee to couple with such a system. But firewalls are increasing in heights such that there are plans in India of using phone apps for the next election [10].

More research needs to be done on the feasibility of protecting robots in factories from outside attack online. PLC was always immune from rogue attacks till the Bashir nuclear plant's (in Iran) Siemens PLC was attacked. The first of its kind PLC virus was somehow planted in the Siemens PLC that controls the plant [11]. Therefore, all big systems like huge oil

Prashobh Karunakaran is an Associate Professor in Electrical Engineering at University of Technology Sarawak (UTS), Sarawak, Malaysia (e-mail: prashobh.karunakaran@gmail.com).

.

and gas establishments are now installing PLC anti-virus protection. Probably McAfee already has solutions to these problems thus researchers do not need to reinvent the wheel[12, 13]. But if the Indian government is currently working on conducting elections with apps in each citizen's smartphone, it is a sign that firewalls are high enough today [14].

II. Literature Review

If two computers are connected to the same router, with the first (server) also connected to a PLC (Programmable Logic Controllers), GE (General Electric) WebView enables triggering the PLC from the second computer [15]. But bringing this concept one step further, which is to trigger the PLC from a computer on the other side of town over the internet requires the factory to have a dedicated static IP address leased from the ISP (Internet service provider). This is costly and in some cases the ISP may not have an IP address available for lease [16].

One way to get around this is to use Dynamic Domain Name Service (DDNS) through a provider like DynDNS.com (there are also other providers like TZO and DMOZ) [17]. This service can dynamically update DNS information as the IP address changes occur on the router. Most modern routers have built-in DDNS clients that support this function. Say a router is connected to a laptop and this laptop is connected to a PLC which controls robots in a factory. Upon signing to the DynDNS service provider, it keeps track of the changes in the public IP address of the router. On the DynDNS account, one can also define an available URL to point to the Public IP address of the router being used for this experiment [18]. As an example, an IP address can be purchased from: https://account.dyn.com. Individual devices on the local LAN including the server laptop used in the experiment can be assigned a port number using port translation done on the firewall. The firewall can be an independent device or may be bundled as a service within the router. For this example, one can assign port 5000 to the internal IP address of the server laptop, one can access the server laptop from another country [19].

In a typical small business or home router there are many services that are bundled into it. Some of these are: Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP) server and the Firewall service. The DNS server translates human readable domain names into IP addresses; for example, www.unimas.com.my is translated to 124.82.253.238 using Internet Protocol Version 4 (IPv4). But even that string of decimal numbers is meant to be human legible. The final transmission is a string of binary numbers. The new protocol currently being implemented is Internet Protocol Version 6 (IPv6) which changes the name to a longer string of hexadecimal numbers designed to cater for the ever-increasing IP addresses cropping up in the world [20].

The DHCP server software is explained as follows; when any network device starts-up and if it does not have a static IP address assigned, it will send out a broadcast using its MAC (Media Access Control) address for an available DHCP server. When the available DHCP server identifies itself, it will send a query to request for the device's MAC address. On receiving this information, the DHCP server will proceed to lease an available IP address to the device. Beyond the router the DNS server translates the Private IP address to a Public IP address [21].

The Firewall server acts as a gate to filter out rogue software and IP addresses from accessing the laptop. So, if 168.74.5.4.2 is the IP address of the PLC server or hub that controls the robots, the Firewall server software must be modified such that the connection from outside to this PLC is allowed [22].

Another important software that resides in a typical router is the DDNS client. The DDNS client informs service providers like DynDNS what its latest IP address is. These providers provide this simple service for free but for similar services with more features, a payment must be made. To view the list of IP addresses for a computer the command, "ipconfig" must be typed in the DOS screen. The DOS screen appears after clicking Start then Run and typing "cmd". It can be noticed that the Default gateway, the DHCP server and the DNS server have the same IP address, because all reside in the same router. The process of pinging is done to determine whether a device or website is responding to a call. Ping google.com means sending a "hello" to Google and waiting for a response. There is always a standard of four replies from the pinged website [23].

III. Methodology and Results

A relay circuit is needed to connect the PLC to the robot as shown in Figure 1. This form of circuitry serves two functions, one is to protect the PLC and the robot, and the other is to overcome the differences in output signals of the PLC and the input signal acceptable to the robot. Some signals are sourcing and others are sinking (for example +24V and -24V respectively).

The GE HMI (Human Machine Interface) helps visualize and control the whole factory. It also has an ability to collect data and sent it to applications that can analyze statistical trends in the production process which often help in deciphering a root cause of problems, thus enabling the removal of these defective products at a faster rate. The defects in products from factories can range from contamination, the wrong habits of some factory workers, electrical problems and mechanical wear-and-tear of machine parts. Thus, this HMI allows an operator or engineer

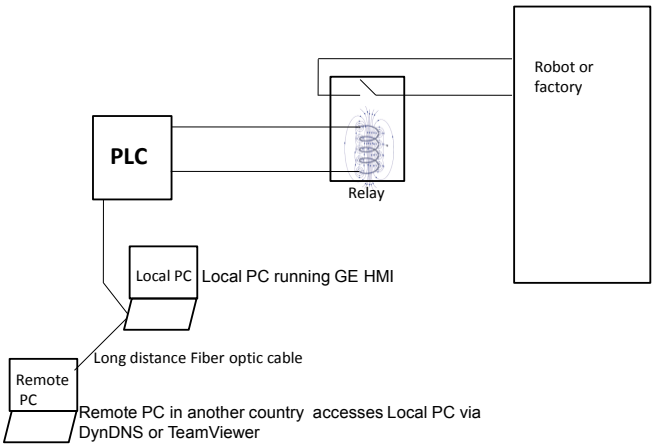

Fig. 1. Schematic depicting the system for remote ordering of products

to make decisions based on the visual data on the computer screen and crunch data with statistical software. There is a built-in software called Historian which enables factory staff to go back in time to find the starting point of a defect in products, even from a home, if they have password access.

In the observations of the operation of the WD factory in Kuching, Malaysia, one can see that if data is viewed at different angles, that is, plotting the charts of parameters (different chemicals, human protocols, or machine mechanical process values) to final yield, root cause can be discovered [4].

The GE HMI enables this, as various views of the production trends can be plotted even during a meeting of engineers compared to the way it is done in WD's Kuching factory where engineersmust come back for another meeting after the numbers are crunched by a human using Excel spreadsheet. With the GE HMI,even the robots can be adjusted in the meeting, over a computer screen to solve some production problems. This HMI can support many hundreds of servers running various portions of a big process [5].

The initial project was to use the GE built-in function to trigger the PLC remotely. This was successfully done as follows. The laptop was connected to the PLC and the GE HMI was used to build a virtual button. This virtual button was programmed to trigger the PLC. The next step is to create a software setting which will turn the laptop into a server. Then from a remote computer, Google Chrome browser was opened and an address, in this case, the address is http://192.168.1.3:8080 was typed in the address bar. The remote computer connects to the laptop server albeit a bit slowly as it starts up, but later the response time is immediate. From the remote computer the same virtual button can be seen and toggling this button with a mouse as shown in Fig. 2, toggles the appropriate output pin on the PLC. The toggling of the PLC from the remote computer happens immediately with no human detectable delay. But this remote computer is also connected to the same router.

Triggering the PLC from a different place was performed, and it was unsuccessful. The reason for this is the requirement of a static IP address from the internet service provider. This is because a bigger router above the small router in the internet network, named DNS, is programmed to change the router's IP address randomly. A static IP address will enable the router to have a permanent address. This will then enable triggering the PLC from another part of town or from another country; effectively enabling customers to trigger factory robots in another country to produce a product. However, these private IP addresses are quite expensive and must be justified by a high factory production output rate to cover its cost [6].

Triggering the PLC from a different place was performed, and it was unsuccessful. The reason for this is the requirement of a static IP address from the internet service provider. This is because a bigger router above the small router in the internet network, named DNS, is programmed to change the router's IP address randomly. A static IP address will enable the router to have a permanent address. This will then enable triggering the PLC from another part of town or from another country; effectively enabling customers to trigger factory robots in

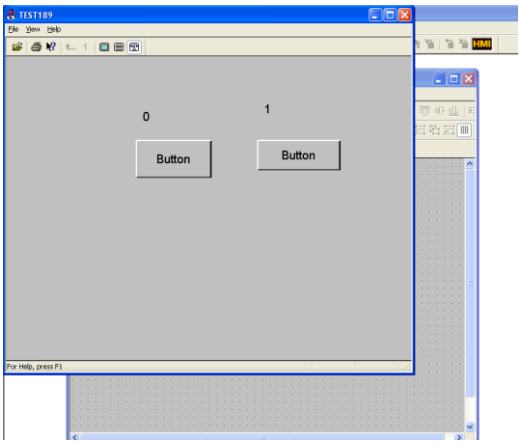

Fig. 2. As the buttons above are clicked in the GE HMI the respective output # 4 is toggled in the PLC

another country to produce a product. However, these private IP addresses are quite expensive and must be justified by a high factory production output rate to cover its cost [6].

Alternatively, a "virtual private IP address", can be set up by registering with www.DynDNS.com. Then a host name must be created by choosing the options, "Host Services" and "Add Host". The next step is to log into the router connected to the laptop and configure DDNS with the same username and password previously set in DynDNS.com. Then a port must be created with forwarding rules in the router to point the port (typically 5000 and over) to the internal IP address of the laptop, typically 192.168.1.10. Thenceforth when accessing the router from another country for example, the address typed should be like http://mypc.dydns.com:5000 [7].

Another approach is to use a remote-control service from entities like TeamViewer and Logmein but these services are potentially more prone to attacks by hackers. More protection software must be built on top of TeamViewer before it can be utilized as a product ordering system. TeamViewer enables remotely connecting to the server computer directly from another country and from there controlling the PLC. This is just like the software used by the GE representatives in China to help in this work. The GE China representative remotely controlled this researcher's laptop in Kuching, Malaysia from his office in Shanghai, China. The GE China representative can see the full screen of this research computer and thereby control the PLC hub. This means he can also control a factory of robots connected to the PLC hub. The TeamViewer website is very intuitive; therefore, setting up the laptop to use this freeware is easy. For a customer to utilize a TeamViewer type software, a logic flow can be after the money has been credited with a credit card, an in-between computer will automatically key in the product specification into the factory's server computer (assuming located in another country), and this will directly instruct the robots to manufacture the required product.

A test was performed using the TeamViewer software, and it remotely (from another part of the town) connected to the server laptop and toggled the PLC which also means triggering a robot to do a sequence of operations is possible for a whole factory of robots.

Once the testing and updating of the HMI screen is finalized, the username and password can be changed. If the PLC output screen toggles by clicking the button on the screen, the software is working well. The next step is to draw all machines, levers and switches on the screen to represent the factory.

The GE HMI is one of the advantages of the GE PLC compared with other common PLCs. Most other PLC software just controls the PLC, and a separate HMI normally comes with the touchscreen. The GE HMI is bundled together with the PLC software. Thus, instead of controlling only the PLC with the software, a whole HMI can be built with the GE PLC software (Proficy HMI SCADA CIMPLICITY 7.5 Workbench). The software can be running on a laptop, and this can control a whole factory. This can be compared to the installation in the Western Digital (WD) factory in Kuching, Malaysia where a touchscreen plus HMI cost about USD2,164 each and there are 64 machines requiring this. This has to be bought in addition to the Mitsubishi PLC which controls the processing machine. Thus for 64 machines the HMI modules cost adds up to about USD421,052. Compared with GE HMI software running on a standard PC can control 64 machines at a cost of just 2% of what WD spent for the HMI system. In addition, GECimplicity replaces the software that is dedicated to acquisition of historical data of events that occurred in the production machines. This will enable easy performance of statistical analysis of the data and thereby ease the production troubleshooting process.

IV. Conclusion

The ability to control a PLC over the internet implies the ability to transform customer's purchase orders immediately into products. This was successfully demonstrated in this work. There is not much literature review on this, probably due to the vested interest in the current purchasing system. The middlemen who get from 30% to 300% markup will not be interested in factories dealing directly with customers. Companies like Amazon have already developed systems where customers trigger actuations in warehouses to start moving products but not to initiate factory robots to produce products. Another notable company that is striving to cut out middlemen is DELL, which sells many of its products directly to customers but still uses humans in-between to process the order. This paper envisages customers who have credited their credit cards triggering factory robots thus greatly reducing wastage in the current purchasing system. But more security software needs to be built on top of this software to enhance security. This is because, if the keystrokes of customers half across the earth can get the robots to function in a factory, rouge customers may also try to hack into the software to destroy the robots either for the thrill of doing this or due to business rivalry. But as mentioned in the introduction, firewalls are high enough that the Indian government is currently working on enabling elections with phone apps.

With the middleman between factories and customers gone, there will be a big increase in the efficiency of the purchasing system which will reduce product costs as there will be no buildup of products due to inaccurate demand prediction.

Reference

[1] Kraemer, K. L., & Dedrick, J. (2002). Dell computer: Organization of a global production network.

[2] Russell, M. A. (2013). Mining the social web: data mining Facebook, Twitter, LinkedIn, Google+, GitHub, and more. " O'Reilly Media, Inc.".

[3] Karunakaran, Prashobh et al. (2022); The Empirical Problems and Solutions of High-Tech Product Manufacturing. IAR Journal of Engineering and Technology (IARJET); ISSN (print):2708-5163, ISSN (online):2708-5155, Vol. 3, Issue 2. DOI: 10.47310/iarjet.2022.v03i02.0032022; 3(2):15-22.

[4] Karunakaran, P., & Osman, M. S. (2013). A study into the feasibility of consumers triggering factory robots to start production over the internet to optimize the current purchasing system. Journal of Manufacturing Engineering, 8(3), 071-074.

[5] Srinivasan, D. (2020). Why Google dominates advertising markets. Stan. Tech. L. Rev., 24, 55.

[6] Shukla, A., Raval, D., Undavia, J., Vaidya, N., Kant, K., Pandya, S., & Patel, A. (2023, February). Deep Learning Applications in Sentiment Analysis. In ICDSMLA 2021: Proceedings of the 3rd International Conference on Data Science, Machine Learning and Applications (pp. 513-519). Singapore: Springer Nature Singapore.

[7] Biswas, B., Sanyal, M. K., & Mukherjee, T. (2023). AI-Based Sales Forecasting Model for Digital Marketing. International Journal of E-Business Research (IJEBR), 19(1), 1-14.

[8] Biswas, B., Sanyal, M. K., & Mukherjee, T. (2023). AI-Based Sales Forecasting Model for Digital Marketing. International Journal of E-Business Research (IJEBR), 19(1), 1-14.

[9] Baviskar, K., Bedse, A., Raut, S., &Darapaneni, N. (2023). Artificial Intelligence and Machine Learning- Based Manufacturing and Drug Product Marketing. Bioinformatics Tools for Pharmaceutical Drug Product Development, 197-231.

[10] Nagarajan, M. K., Kumar, B. P., Teja, N. K., Rohith, M. V., & Babu, N. M. (2023, May). Innovating Elections Smart Voting through Facial Recognition Technology. In 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 877-881). IEEE.

[11] Datta, P. M., & Acton, T. (2023). Did a USB drive disrupt a nuclear program? A Defense in Depth (DiD) teaching case. Journal of Information Technology Teaching Cases, 20438869231200284.

[12] Singh, B. (2023). An Analysis of Cybersecurity in Industrial Automation.

[13] Villanueva-Miranda, I., & Akbar, M. (2023, December). Analyzing Threat Vectors in ICS Cyberattacks. In 2023 IEEE International Conference on Big Data (BigData) (pp. 1368-1373). IEEE.

[14] Putra, R. T., Taufiqurrahman, D. R., & Sagala, K. J. H. (2023). E-Voting System for Election with Mobile Based Apps. International Journal of Research and Applied Technology (INJURATECH), 3(1), 69-78.

[15] Hidayat, A., Nandika, R., Anton, A., Alfitri, N., &Trinanda, A. (2023). Application of hart concentrator to save the number of input analogue channel usage in PLC PAC system on SCADA cimplicity. JECCOM: International Journal of Electronics Engineering and Applied Science, 23-33.

[16] Baltra, G., Song, X., & Heidemann, J. (2024, March). Ebb and Flow: Implications of ISP Address Dynamics. In Proceedings of the Passive and Active Measurement Conference. Springer.

[17] Bruen, O. G. (2024). WHOIS RunnIngtHeInteRnet.

[18] Okuthe[1], J. A., &Terzoli, A. (2023, June). Check for updates Assessing the Impact of DNS Configuration. In Towards new e-Infrastructure and e-Services for Developing Countries: 14th EAI International Conference, AFRICOMM 2022, Zanzibar, Tanzania, December 5-7, 2022, Proceedings (Vol. 499, p. 76). Springer Nature.

[19] Hsu, Yuan-Ying and Tseng, Chien-Chao (2005). Prime DHCP: A Prime Numbering Address Allocation Mechanism for MANETs. IEEE Communications Letters Vol 9, No.9.

[20] Shrestha, P., & Sherpa, T. D. (2023, January). Dynamic Host Configuration Protocol Attacks and its Detection Using Python Scripts. In 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF) (pp. 1-5). IEEE.

[21] Gowda, S., & Dayananda, R. B. (2023, July). Detection And Prevention of ARP Attack in Software Defined Networks. In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-5). IEEE.

[22] Gaur, V. S., Sharma, V., & McAllister, J. (2023). Abusive adversarial agents and attack strategies in cyber- physical systems. CAAI Transactions on Intelligence Technology, 8(1), 149-165.

[23] Perone, S., Faramondi, L., &Setola, R. (2023, July). Default Credentials Vulnerability: The Case Study of Exposed IP Cams. In 2023 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 406-411). IEEE.