PLC NETWORK SECURITY (ATTACKS AND PROTOCOLS)

Muhammad Hadin Sami* and Sarmad Hameed**
*(Department of Mechatronics Engineering, SZABIST University, Karachi, 7590, Pakistan
Email: msme20107107@szabist.pk)
**(Department of Mechatronics Engineering, SZABIST University, Karachi, 7590, Pakistan
Email: sarmad.hameed@szabist.pk*)

Abstract:

Programmable Logic Controller (PLC) is one the major controlling device in automation system. PLC (Programmable Logic Controller) is used to control heavy machinery and its network security is very important as loss of secure data can cause great loss to the industry. Many researches and existing work in PLC (Programmable Logic Controller) network security have failed to make it enough secure to stop the attackers from attacking and destroying the program and secure data. In order to extend the research, worked on PLC security and tested the attacks caused on the PLC and tried to secure the network by extending the network security programming. Tested the PLC (Programmable Logic Controller) using a testbed and applied five network attacks which were seriously affecting the Programmable Logic Controller. In this paper four attacks are worked on Replay Attack, MITM also known as Man in the Middle, Stealth Command Modification and Payload Attack.

Keywords -- PLC (Programmable Logic Controller), MITM, Protocols, Security, Intruders, Cyber Security, Attacks.

I. INTRODUCTION

Programmable Logic Controller is one the major controlling device in automation system. PLC is used to control heavy machinery and its network security is very important as loss of secure data can cause great loss to the industry. There are two types of Programmable Logic Controller (PLC), first compact PLC and the second is module PLC. Compact PLC is used for low profile machinery like garments machinery. Module PLC is used on power plants and engineering work stations. The security of both the PLCs is same and thus a major issue to be resolved is network security so that the PLC becomes more secure and no intruders can change the programming. PLC programming uses ladder logic. Both PLCs have the same logic but the difference is that in compact PLC we use simple ladder logic whereas in module PLC we add separate module for each component of a workstation. After knowing the two types of PLCs we must be clear of the concept of network security of the PLC. The PLC is connected to the Ethernet and thus this how the attackers attack the PLC. PLC Network security uses protocols such as Modbus, DNP3 and etc. To keep the network secure from intruders, a testbed was created to solve the

problem and complete the research. The five attacks worked on are Replay Attack, (MITM), Stealth command modification and Payload Attack. In Replay Attack the intruder breaks the privacy using software's and the command user sends it retypes it multiplies many times causing to distort data. Secondly Man in the Middle which causes a bug in the PLC creating a lag in PLC or can crash it completely which can cause a great loss to the industry. Thirdly, Stealth command modification changes the program in the PLC which can damage our machinery indeed causing a great loss. Fourth is the Payload attack in which the attacker does some malicious activity to harm the network security.

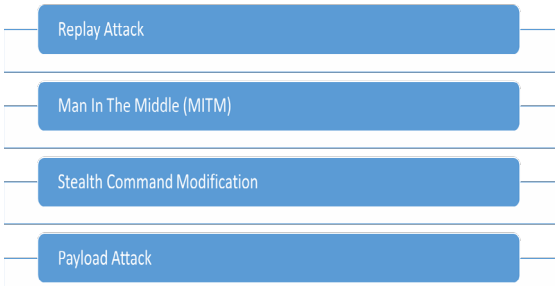

Figure 1: Four Attacks

The paper is formatted and written as follows. In the first part we gave the background of the PLC (Programmable Control Logic). In The second half we gave the details of PLC, their ways of communication with other work stations and the securities which needs to be considered. In the second last part we talked about the different attacks. Finally, we provide a conclusion.

II. BACKGROUND

Programmable logic controllers with the abbreviation PLC were made in the late 1960s. Machine Control systems that are relay based were used in the major U.S. vehicle manufacturing space thus to replace them PLCs were created. Relay based control systems back than were difficult to handle and not very user friendly. Majority of the automation and manufacturing industries disliked it.

In 1968, Modular Digital Controller was designed by Dick Morley of Bedford Associates in Massachusetts later dubbed the mod icon. The mod icon 084's innovation bought light to the field and relay- based control systems became outdated. Many Control functions of high-level complexity are easily carried out by the PLCs. PLCs are user friendly microprocessor based special computers. They are designed to persevere unforgiving and strenuous circumstances such as in warmed, cooled and indeed damp situations. Utilized for mechanization ordinarily within the mechanical created area. Programmable Logic Controllers are programmed the type of computers which are programmed and tackle the machinery operations, commonly the power station, distribution systems, power, generation systems and gas turbines

A computer language is used to program the PLCs. PLC programs are first written on the computer and then copied to the PLC using a cable. The program transferred to the PLC is stored in the memory of PLC. The logic is usually interchanged with the program inserted by the operator during the change happening in amongst the relay control and PLC. Advantage of PLC have been taken by the manufacturing and process control industries ever since it is created leaving behind the mod icon. In order to store specific functions PLC use built in programmable memory.

III. RELATED WORK

Various examination papers detail network assaults on SCADA frameworks. The vast majority of existing work centers around contemplating assaults on Modbus convention [1], contemplated as one of the most settled organization conventions for Mechanical Control Frameworks. Huisting et al. proposed a thorough scientific categorization of assaults focusing on the Modbus convention. In excess of 200 assaults were accounted for and momentarily talked about covering the two variations of Modbus, to be specific, the Sequential variation and the TCP variation. Albeit the scientific classification was thorough, no assault has been executed nor tried. Subsequently, for the majority of the recorded assaults.

There is no assurance that they are feasible in practice.

The nearest work to our own was introduced By Beresford [2], in which a few assaults on the correspondence accounted amongst designing station and PLC. Beresford referenced few attacks which can be relevant on Siemens Programmable Logic Controller S7-1200 and S7-300, an example records recovery, relay assault and dispatching a faraway shell on a PLC. Notwithstanding, via way of means of giving introduced attacks a shot our putting. The explanation is that the PLC firmware is commonly much easier to use and much safer firmware applied withinside the Beresford's investigations. Also, replay assault is likely to be much way better "instinctive" than the Beresford's since a number of bundles that are recorded are essentially replayed after a reaction from the Programmable Logic Controller. Beresford's replay assault consolidates in sending all of the recorded bundles gathering without considering any reaction from the Programmable Logic Controller. [3]

A. Programmable Logic Control (PLC)

Programmable Logic Controller is a vital aspect in current Industrial Control Systems (ICS) precise in SCADA systems. A PLC is a unique reason PC meant to supplant hand-off forums and manipulate a real cycle. Figure 3 gives the general gadget and programming layout of PLCs. There are some tremendous attributes that apprehend PLCs from person PCs: PLCs are meant to paintings in brutal c rrent situations and are changed in switch stepping stool intent or different PLC programming dialects. Also, a PLC executes a simple payload application in a successive style. Once dispatched in an ICS, a PLC continuously gathers readings from sensors related to it reasserts of info, runs the PLC payload application, furthermore, creates yields that manipulate the real cycle. As seemed in Fig. 2, PLC manipulate application may be created on designing workstations making use of programming that upholds steppingstool intent or different PLC programming dialects also, downloaded to goal PLC for execution. Administrator of an ICS may also display screen and manipulate the real cycle with the aid of a human-gadget interface (HMI), which speaks with PLCs to get ongoing interplay statistics and difficulty manipulate orders.

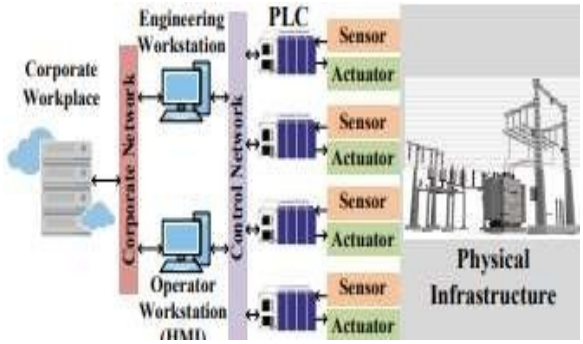

Figure 2: Designing Workstations

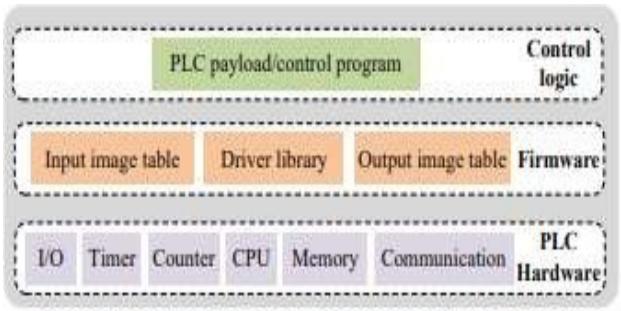

Figure 3: Gadget and Programming Layout of PLC

To manage and display screen real cycle, a PLC's firmware executes records and yield photograph tables simply as a application test cycle. An application test cycle contains of data filter, application look at, yield output, and housework stages, which can be seemed in Fig. 4. After framework hearthplace up, a PLC constantly strolls thru the 4 intervals of this system test cycle as follows: First, withinside the records look at stage, the PLC Equipment I/O Clock Counter critical processor Memory Correspondence Info photograph desk Driver Library Yield photograph desk Firmware Control cause PLC

payload/manage application

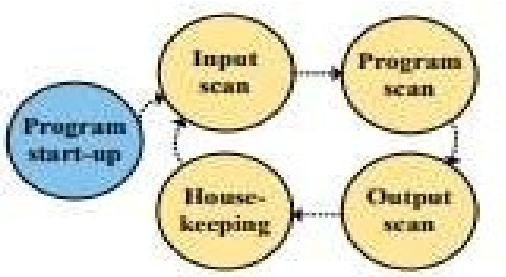

Figure 4: Application Test Cycle

PLC firmware examines the I/O pin esteems and thinks of them into the data image desk. At that point, withinside the application test degree, suggestions withinside the payload application is carried out personally utilizing values put away withinside the statistics image desk. Yield esteems are created for the duration of this degree and composed into the yield image desk. Then, withinside the yield clears out degree, values withinside the yield image desk is moved to the out of doors yield terminals, making manipulate sports indicated withinside the payload application take impact. At lengthy last, withinside the home tasks degree, internal minds reminiscence and framework hobby are performed. Moreover, correspondence needs started from exceptional hosts (e.g., the HMI) or created via way of means of the payload application itself are furthermore overhauled earlier than the subsequent undertaking look at cycle begins. [4]

B. PLC Security and Cybersecurity

As protection issues live in several professional areas together with the manufacturing line automation space, getting up to velocity along the diverse kinds of Programmable Logic Controller Security which is basic. By making and executing a success method to live secure, you'll in all likelihood avoid troubles, vacation, and misfortunes. Understanding the diverse types of PLCs may be surprisingly beneficial whilst investigating PLC protection. PLC Cybersecurity is essentially how the manage community is related to the internet, in addition to different networks. Incident response planning and plans, issues drafting and revising policies, issues drafting and evaluating procedures, and the retention of cybersecurity experts and vendors are just a few of the PLC issues. In addition, there is a demand for breach exercises, instruction, and breach simulations. One of the most important studies is the need for cybersecurity policy review and advice. A call for file control and records infrastructure. Privacy hazard control and Assessment of cybersecurity hazard in mergers and acquisitions is one factor of PLC protection.

C. PLC Attacks and Testing

PLC is attacked by various type of attacks out of which many are discovered and many are to be explored learned and worked on. The PLC testing is basically checking which attacks are working on the PLC even after applying network protocols. We test that which are the PLC network security attacks and how to sort out the attacks by applying more protocols.

1) Replay Attack:

A replay ambush (also called playback attack) may be a shape of community ambush wherein true-blue data transmission is maliciously or falsely rehashed or postponed. This could be done by the originator or by an enemy who intervention the information and re-transmits it, most likely as portion of a spoofing assault utilizing IP parcel substitution. This can be one of the lower-tier man-in-the-middle ambush variations. The larger part of replay ambushes is inactive in nature.

A way to describe such an assault is: "An assault on a security protocol using the replay of messages from a different context into the intended context, so deceiving the serious participant(s) into believing they've successfully completed the protocol run. ."Replay assault comprises of 3 stages: beginning a PCS7 order (stop, start, and so forth), catching the bundles, and replaying the caught parcels sometime in the not-too-distant future. The caught parcels relating to a provided order are first prepared by sifting through any bundles that are not part of the orders. Since PCS7-PLC correspondence makes use of the COTP convention (port 102), a few different bundles are sifted through. Simply parcels withinside the PCS7-PLC ways are endorsed (bundles withinside the inverse direction is sifted through).

Wiped clean visitors for every order are then position away in a pcap file. At first, tcp replay suite is applied to replay the parcels. Tcp replay accompanies diverse instruments, as an example, tcp prep (parcels pre-processor that secludes bundles in the direction of each path), tcp rewrite (pcap report editorial supervisor which reworks parcel headers), tcp replay (replays pcap statistics onto the community), and so on Utilizing those devices the pcap report is pre-organized previous to replaying with the aid of converting the supply IP and recalculating the check sum esteem in every package deal. When preprocessed pcap report is then replayed at the PLC, a huge part of bundles is disposed of with the aid of using the replay attack fizzles and PLC. The parcels are disposed of 2 essential reasons. To begin with, the association SEQ and confirmation ACK) numbers withinside the parcels that are replayed remain unchanged. Thusly, TCP/IP element on PLC labels are the bundle copies and disposes of them. Second, tcp replay is the tool that replays the bundles withinside the pcap file always without pausing the PLC from any response. The PLC will now obtain some bundles from the top organization and dispose of them. In the past this problem was noticed with the aid of using Maynard et al. [6]. The aid of using the TCP/IP element to beat those problems and to make certain that the replayed parcels are stated.

PLC, we grew to become to compose a changed python content material making use of scapy. Scapy is a super parcel manage application written in python and as a result may be efficiently applied in python contents. It includes a number of parcel management capabilities, such as sniffing and replaying packages within the organization, community checking, tracerouting, and so on. In any case, the foremost valuable scapy highlights for our replay assault are the capacity to alter affiliation and affirmation numbers, as well as the capacity to arrange needs and answers. Managing the reproduction succession and confirmation numbers accommodates of reevaluating those number and converting them with the help of scapy. Controlling package deal by making use of Scapy which is apparent due to the fact that any package deal discipline is largely to be held with the aid of using the dab administrator (as an example ip.src, tcp. Flags, rcv [TCP]. seq).At first, abnormal grouping and confirmation numbers are picked. At that point, at each parcel sending, the numbers are accelerated furthermore, introduced to the subsequent package deal.

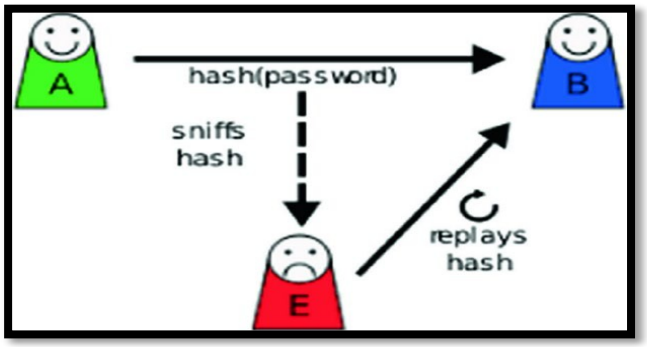

Figure :5 Replay Attack

2) Man in the middle attack:

A man-in-the-middle (MITM), monster-in-the-middle (MIM), machine-in-the-middle (MIM), monkey-in-the-middle (MITM), or person-in-the-middle (PITM) assault could be a cyberattack in which the aggressor furtively transfers and likely modifies communications between occasions who accept they are at the same time talking with each other. Dynamic spying is an illustration of an MITM assault, in which the assailant builds up free associations with the casualties and transfers messages between them, driving them to accept they are spearmen at once to each other over an individual association, when in reality the complete verbal trade is overseen by implies of the aggressor. The assailant ought to be able to caught all important communications sent between the two casualties and supplant them with fresh ones. Typically straightforward in numerous occasions; for illustration, an assailant within the gathering run of a decoded Wi-Fi get to point ought to act as a man-in-the-middle.

A MITM assault can be effective best when the aggressor mimics each endpoint adequately well to coordinate their desires, as its objective is to sidestep common authentication.

To protect you from MITM attacks, most cryptographic protocols include a few different types of endpoint authentication. TLS,for example, can authenticate one or all events using a certificate authority that is dependent on each other.

The correspondence among PCS7 and the PLC employments are using COTP on the Ethernet. The Ethernet is a conference that makes use of ARP. Hence, the defense is useless towards the attack MITM attacks via ARP. In an exchanged Ethernet employer, a bunch X tries its best to talk with a bunch Y (with a found-out IP cope with) desires its real location (Macintosh). The Mac address can be gotten by sending out an ARP requesting to all has interior the organization. In a ordinary circumstance, have Y will react with the correct IP Mac pair.

During an assault, a comparative employer's attacker will send a fake reaction with a false IP-Macintosh claiming to be the proprietor of Y's IP address. Ordinarily, the aggressor surges the manager with its wrong reply, causing the casualty have (X) to disregard around the right one conveyed through have Y and center on the counterfeit coordinate. ARP harming is as often as possible dispatched in the midst of has, permitting the attacker to insert himself as a entry between the two casualties and sniff all bundles among them sooner or afterward. In our case, an ARP harming MITM assault is carried out between the PCS7 and the PLC by means of the Ettercap instrument. [5].

The attack is successful, as the aggressor has burrowed all of the bundles transacted between the PCS7 and PLC (Kali). MITM attacks can be static or dynamic. An inactive version involves simply noticing the PLC's site visitors and so compromising the confidentiality of orders dispatched from the PLC. A working adaptation is more perilous since it permits the aggressor to alter with the bundles and orders, as well as mess with the framework's ordinary exercises. [3]

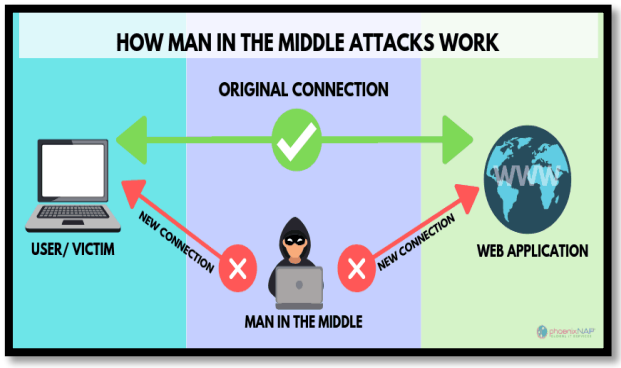

Figure :5 Man In The Middle (MITM)

3) Stealth command modification attack:

MITM and Replay Assault are combined in the Stealth Command Modification attack. Attacks which objectives sniffing the visitors among the PCS7 and PLC, later on meddling with dispatched orders with the aid of using replaying different orders in a secrecy way. By using this attack, the attacker can completely change the nature of SCADA framework for the reason that sending an order activates the execution of some other order. The attack studies three precept steps: MITM attack, order identification, and replay attack of a bogus order. At first, the assailant (Kali) starts off evolved with the aid of using dispatching MITM attack to position among the PCS7 also the PLC exactly as portrayed withinside the beyond segment. At that point, it remains in an inactive kingdom noticing the visitors latently and sitting tight for orders dispatched with the aid of using the PCS7 host to the PLC (Stage 1). For order reputation withinside the corporation, Grunt interruption reputation framework (IDS) [19] is utilized. Grunt is a signature- primarily based totally corporation IDS which allows to differentiate designs of visitors withinside the corporation. At present, Grunt is designed to stumble on varieties of commands, namely, begin and prevent. As quickly because the aggressor acknowledges an order from the PCS7 host to the Programming Logic Controller (Stage 2), an extrude order might be replayed to the Programming Logic Controller (Stage 4). That is, if a starting order is identified, the aggressor replays a prevent order to the Programming Logic Controller. On the off risk that a prevent order is recognized, the aggressor replays a starting order (with an extrude PLC program1) to the PLC.

Nonetheless, it isn't hard to look that at the off risk that the assailant meddles with a starting order to make it a prevent order (or the inverse), the PCS7 will swiftly see that something is not right. To make the attack as secrecy as ought to definitely be expected, the assailant proceeds with the correspondence with the PCS7 have at the same time as mimicking the PLC (Stage 3). So, for the PCS7 have the correspondence has all of the earmarks of being absolutely common. To be beyond any doubt, to create the assault mystery, Stuxnet record common repeat regards. At assault time it is performed that the ones recorded frequencies to create the checking framework accepts that rotators are running as common [2,3]. ambush may be a blend of replay and MITM ambushes which targets the activity between the PCS7 and PLC and a short time later interfering with sent orders by replaying other orders in a mystery way. Through this ambush, an enemy can completely alter the conduct of the SCADA system since sending an arrange prompts the execution of another arrange. The ambush encounters three central steps: MITM ambush, arrange distinguishing proof, and replay of a fake arrange. At first, the aggressor (Kali) dispatches an MITM assault to put himself between the PCS7 and the PLC, as appeared within the past scene. At that point, it remains sit still, watching activity imperceptibly and holding up for orders from the PCS7 have to the PLC (Stage 1 in Fig. 3). Snort intrusion acknowledgment system (IDS) [19] is utilized within the organization for order recognition. Snort could be a signature-based organization IDS that permits for the recognizable proof of activity designs inside the company. As of now, Snort is as it were able of recognizing two sorts of commands: begin and halt. A substitute arrange will be replayed to the PLC as before long as the attacker recognizes an arrange from the PCS7 have to the PLC (Stage 2). In other words, if a commencement order is found, the aggressor sends a stop order to the PLC. On the off chance that a stop order is recognized, the aggressor replays a beginning order (with an alternate PLC program1) to the PLC.

Nonetheless, it is not difficult to see that on the off chance that the assailant meddles with a beginning order to make it a stop order (or the inverse), the PCS7 will rapidly see that something isn't right. To maintain the highest level of concealment possible, the assailant continues his correspondence with the PCS7 while imitating the PLC (Stage 3). As a result, the correspondence for the PCS7 bears all the hallmarks of being entirely conventional. Stuxnet used this strategy in its well-known attack on Iran's nuclear facility. To be sure, Stuxnet logged typical recurrence esteems in order to keep the attack secret. Then, throughout assault time, it played those recorded frequencies to convince the checking framework that the rotators are functioning normally. [2,3].

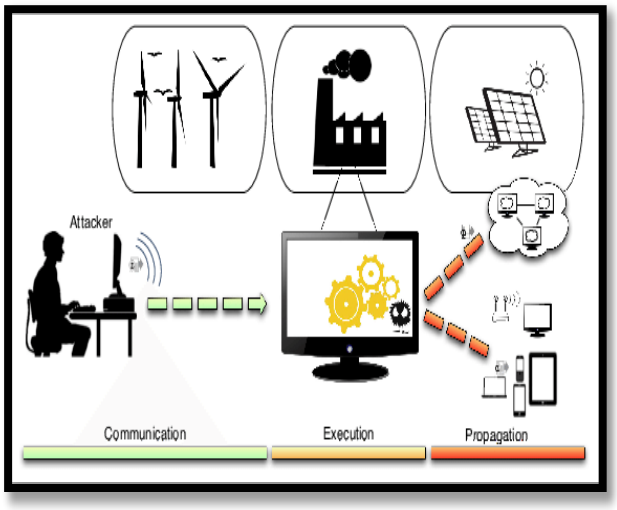

Figure :6 Stealth Command Modification

4) Payload Attack:

A malicious payload is an assault factor answerable for executing a pastime to damage the target. Some not unusual place examples of malicious payloads are worms, ransomware, and different malware that arrive on computer systems with the aid of using clicking awful hyperlinks or downloading dangerous attachments.

Malicious payloads can motive facts deletion, encryption, and exfiltration. In a few cases, chance actors encrypt payloads to preserve their malicious code hidden from antimalware solutions.

Utilizing manipulate framework determinations, runtime behavior version of real PLC payload software is installation and placed away withinside the PLC firmware. The condition connections among records reasserts and yields, the amount of company parcels created after numerous manipulate activities, simply as timing connections among I/O and company occasions,

are displayed. By changing the PLC firmware, runtime practices of the payload software (e.g., I/O and company get entry to designs) are time- stepped and analyzed in opposition to the set-up runtime behavior version. Likewise, a reinforcement shape of the yield photograph desk is independently placed away via way of means of the firmware towards the begin of every software has a look at cycle. In the occasion that a particular anomalous runtime behavior is prominent, the reinforcement yield photograph desk is stacked to overwrite the yield created via way of means of the payload. Accordingly, any yield diagnosed with the prominent anomalous runtime behavior may not have an effect on the real framework. For PLC payload sending/accepting community bundles, community needs are moreover impeded whilst a runtime behavior abnormality is identified via way of means of the firmware.[7]

D. Resolving the Problem

We check the PLC is secure or not after applying our new protocol system. This part gives the rundown of open examination zones that actually remain less examined dependent on the significant divisions made previously: Assault explicit Security Weaknesses in IoT:

- Creating lightweight cryptographic conventions to secure IoT gadgets against weak assaults.
- Creating preventive methods against Traffic Examination assaults. Tying down RPL to deal with the issue of directing circles or forestalling change of directing data.
- Creating preventive measures to battle sinkhole and wormhole assaults in an IoT framework.
- Proposing methods or answers for forestall or settle network DDoS assaults. Lightweight Enemy of Malware arrangements should be contrived to ensure the IoT gadgets from Malware.
- Creating lightweight plans to at the same time give information security while keeping up availability to just approved clients.
- Need for creating lightweight cryptographic calculations and productive key administration plans for securing information privacy furthermore, uprightness key administration plans for securing information privacy furthermore, uprightness.
- Creating application explicit information assurance strategies is of critical need. For instance, medical services framework requires legitimate access control systems to give assurance to delicate wellbeing records nonetheless, if there should be an occurrence of VANET keeping up information respectability and secrecy is of highest need.

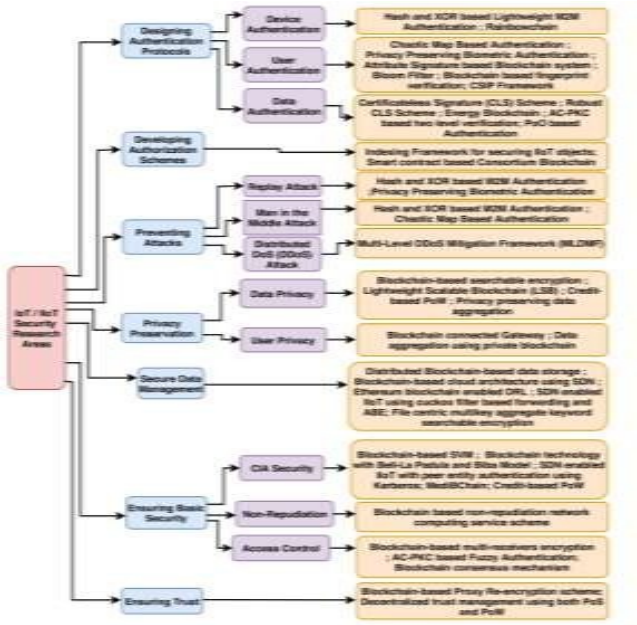

Figure:7

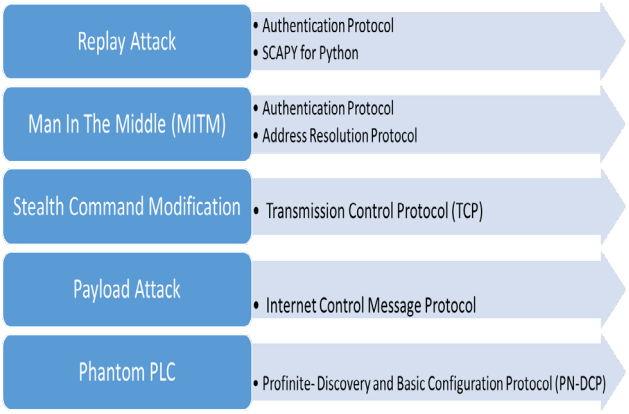

Figure: 8

1) Security Issues in IIoT:

- Planning a protected Haze based IIoT design to diminish criticism inactivity and calculation overhead on asset obliged gadgets.
- Getting all cloud-based communications in a modern climate. This incorporates information moved and put away in the cloud.
- Tying down all gadget-to-gadget interchanges in IIoT from assaults like altering.
- Planning security calculations in a manner to dispose of trust on third party cloud specialist co-ops completely.
- Creating application explicit assault counteraction plans for IIoT conditions like Brilliant Manufacturing plants, Shrewd Frameworks and so forth
- Building up a typical and normalized security strategy for all IoT gadgets from various sellers in a mechanical setting.
- Planning versatile and dynamic blockchain-based security system for both very good quality workers and low fueled IoT gadgets.
- Need for creating energy proficient blockchain agreement calculations in view of energy requirement IoT gadgets, regularly mechanical hardware [8]

IV. SUMMARY AND FUTURE WORK

PLC network security can never be resolved at any stage of life because how much ever we modify the security protocols their attackers find a way to breakthrough; hence this problem remains unsolved despite of excess research in this field. The entirety of the introduced assaults expect admittance to the ICS measure control organization. Be that as it may, as exhibited by Stuxnet and the Ukraine electric network assaults, complex assailants can ultimately gain admittance to such networks. Consequently, the generally "air- gapped" measure control organization will just give a bogus sense of security to the administrators. It is shown that, by utilizing different methods, framework administrators might be misled towards designing the off- base PLC, or might be precluded to associate with the PLCs utilizing the TIA gateway. The effect of such assaults would rely upon the explicit ICS; however, an interruption of actual cycles is a conceivable result. Organization safety efforts, as firewalls and interruption discovery frameworks, could forestall a portion of the adventures referenced in this paper, for model, identifying unreasonable or obscure ARP bundles. Notwithstanding, abuses that use real usefulness, like the one referenced in area on a tainted designing station in the network, would in any case be fruitful since these correspondences can't be hindered because of the real controls that TIA entryway requires. An administrator won't interface with the influenced gadgets and the undermined machine could start another meeting regardless of whether the PLC has been bodily reset. Besides, it became found that the S7-ACK parcel, which would not want trustworthiness or verification subtleties withinside the bundle, has the ability to be misused. A viable comfort might be a firmware replace of the PLCs, on which PLCs will disengage any inactive S7 assembly after sure timeframe. Notwithstanding, if the aggressor has the potential to replay parcels with the proper interaction and trustworthiness bytes, actual S7 affiliation ought to anyhow be disregarded if some other affiliation is beginning out after the break.

Future paintings will contain assembling greater records at the highlights and weaknesses of the S7CommPlus conference and comparative conventions from diverse merchants. An exam on how these weaknesses may be misused will likewise be performed, specifically the ones were given from exam of the TIA entryway. Furthermore, the creators be given there are exchange methods to misuses the PN- DCP conference, like a CVE that became as of overdue disbursed that encouraged maximum Siemens PLCs (Data Innovation Research center, 2018).

A research will likewise be executed on distinguishing methods to enhance the safety of the manage

frameworks. One ability direction is to accumulate an inexpensive honeypot. The honeypot can, both effectively (sniffing the network) or latently (sitting tight for an affiliation) distinguish whether or not an affiliation is from a authentic TIA front or an aggressor's undertaking to misuse actual functionalities. Unexpectedly, the extra a part of the abuses referenced on this paper, as an example the ghost PLC, and the records obtained through flip round designing the TIA front is essential for creating a honeypot that acts like an authentic PLC. Besides, it might be high-quality for the commercial enterprise to have a progressed norm at the correspondence conference this is accountable for the affiliation among designing programming and PLCs. [9]

V. CONCLUSION

Taking everything into account, when a security break happens, paying little mind to the particulars. Believing who approaches a control frameworks climate and thumb drive is essential. In the event that somebody approaches the control framework climate and thumb drive, guarantee they're capable and up-to-speed with their group or potentially organization.

PLC network security was tested by checking the attacks and solved it by applying new network protocols. PLC network security can never be resolved at any stage of life because how much ever we modify the security protocol the attackers find a way to breakthrough hence this problem remains unsolved despite of excessive research in this field.

ACKNOWLEDGEMENT

We would like to thank our university SZABIST to teach us with a positive attitude and a motivating us to publish our paper in a conference. It would not have been possible without the support of our teachers and faculty of the university

REFERENCE

[1] M. Organization, Modbus protocol specification
[2] D. Beresford, Exploiting Siemens Simatic S7 PLC, Black HatUSA (2011)
[3] Asem Ghaleb a , Sami Zhiouaa,∗ , Ahmad Almulhemb, On PLC network security , King Fahd University of Petroleum and Minerals (2018)
[4] Huan Yang, Liang Cheng, and Mooi Choo Chuah, Detecting Payload Attacks on Programmable Logic Controllers (PLCs), Lehigh University
[5] P. Maynard, K.M. Laughlin, B. Haberler, towards understanding man-in-the-middle attacks on IEC 60870-5-104 SCADA networks, in: Proceedings of the Second International Symposium on ICS & SCADA Cyber Security Research, ICS-CSR, 2014, pp. 30–42.
[6] S. Zonouz, J. Rrushi, and S. McLaughlin, "Detecting Industrial Control Malware Using Automated PLC Code Analytics," IEEE Security & Privacy, vol. 12, no. 6, pp. 40–47, November 2014.
[7] Jayasree Sengupta a, ∗, Sushmita Ruj b, Sipra Das Bit a, A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT, 2020
[8] Investigating Current PLC Security Issues Regarding Siemens S7 Communications and TIA Portal Hui ● McLaughlin
[9] A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke, Scada security in the light of cyber-warfare, Computers & Securityvol. 31(4) (2012) pp. 418–436.
[10] N. Falliere, L. Murchu, E. Chien, W32.Stuxnet Dossier,
Symantec Security Response(2012).
[11] S. Zhioua, The middle east under malware attack: Dissecting cyber weapons, Proceedings of the IEEE ICDCS Workshop on
Network Forensics, Security and Privacy (NFSP) (2013).
[12] D. Beresford, Exploiting Siemens Simatic S7 PLC, Black
HatUSA (2011).
[13] P. Huitsing, R. Chandia, M. Papa, S. Sheno, Attack taxonomies
for the Modbus protocol, International Journal of Critical Infrastructure Protection 1(0) (2008) 37–44.

[14] W. Gao, T. Morris, B. Reaves, D. Richey, SCADA Control System
Command and Response Injection and Intrusion Detection,eCrime Researchers Summit (eCrime)(2010) 1– 9.
[15] L. Pietre-Cambacedes, M. Tritschler, G. Ericsson,
Cybersecurity myths on power control systems: 21 misconceptions and false beliefs,IEEE Transactions on Power
Deliveryvol. 26(1) (2011) pp. 161–172.
[16] Y. Yang, K.M. Laughlin, T. Littler, S. Sezer,
E.G. Im, Z. Yao, B.
Prang-gono, H. Wang, Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid scada systems, Proceedings of the International Conference
on Sustainable Power Generation and Supply (SUPERGEN) (2012) pp. 1–8.
[17] T. Morris, W. Gao, Industrial control system cyber attacks,
Proceedings of the First International Symposium on ICS & SCADA Cyber Security Research, ICS- CSR(2013) pp. 22–29.
[18] P. Maynard, K.M. Laughlin, B. Haberler,
Towards understanding man-in-the-middle attacks on IEC 60870-5-104 SCADA networks, in: Proceedings of the Second International Symposium on ICS & SCADA Cyber Security Research, ICS-CSR, 2014, pp. 30–42.
[19] M. Organization, Modbus protocol specification
[20] K.M. Laughlin, S. Sezer, P. Smith, Z. Ma, F. Skopik, PRECYSE:
Cyber-attack detection and response for industrial control systems, Proceedings of the Second International Symposium on ICS & SCADA Cyber Security Research,
ICS-CSR(2014) pp. 67–71.
[21] A.G. Siemens, The simatic PCS7 process control system brochure, April 2013.
[22] Network Working Group, ISO transport protocol specification
(RFC 905), April 1984.
[23] G. Devarajan, Unraveling SCADA protocols: Using sulley
fuzzer, Proceedings of the DEFCON Fifteenth Hacking Conference(2007).
[24] P. Biondi,Scapy, http://www.secdev.org/projects/scapy.
[25] A.a. NaGA, Ettercap, http://ettercap.sourceforge.net.
[26] M. Roesch, Snort: Lightweight Intrusion Detection for
Networks, LISA vol. 99(1) (1999) pp. 229–238.
[27] R. Gerhards, The syslog protocol (RFC 5425), March 2009