2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST) | 978-1-6654-2404-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICAICST53116.2021.9497829

Security Challenges in Industry 4.0 SCADA Systems – A Digital Forensic Prospective

Varun Rakesh Malik*[a], Gobinath K[#b], Santosh Khadsare[$c], Ajay Lakra[^d], Subodh V Akulwar[&e]
Thapar Institute of Engineering and Technology[a],
Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology[b,c,d,e]
vmalik_be17@thapar.edu*, gobinathk@cert-in.org.in[#], satntoshkhadsare@gmail.com[$], a.lakra@nic.in[^], sakulwar@meity.gov.in[&]

***Abstract*—Industry 4.0 is that the digital transfiguration of production and connected industries with worth creation processes called smart factory. The building blocks of Industry 4.0 are fusion of Cyber Physical systems, Artificial Intelligence, Robotics, cloud computing and the Internet of things(IoT). In Industry 4.0, the Supervisory Control and Data Acquisition (SCADA) systems performs more intelligence, automation and self-learning with the centralized technologies. With these, the SCADA controls manufacturing processes in industries by monitoring, gathering and processing of real time data. At the time of making a product through Industry 4.0 in any factory, if any faults occurred in the Supervisory systems, the entire system gets collapsed and leads to harmful to consumers. The advanced digital forensics techniques for the entire Industry 4.0 architecture are needed to identify the errors in the real time processes and new tools to be designed to ratify during live processes. In this work, some of the forensics challenges in the SCADA systems of Industry 4.0 and the available digital forensics tools for live systems are discussed with possible proposed solutions. It also discusses the limitations and difficulties faced in digital forensics of Industrial Control Systems.**

***Keywords*—Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), Industry 4.0, Internet of things (IoT), Digital Forensics.**

I. INTRODUCTION

The 4th phase of the Industrial Revolution (Industry 4.0) has led to a focus shift in industry practices towards automation and going wireless. Also called Industry Internet of Things (IIoT), Industry 4.0 focuses on automating systems, facilitating real-time data access and achieving better interconnectivity between systems [18, 19]. It wants to achieve an integration of physical production and operations by employing smart digital technology, machine learning and the internet of things, resulting in a better connected ecosystem for manufacturing and supply chain management companies [21, 27].

These new proposals have come with their share of associated issues that need to be tackled. For instance, with Industry 4.0, the industrial processes are all done over networks. This has increased the intensity of attacks especially on systems like ICS (Industrial Control Systems) and SCADA (Supervisory Control and Data Acquisition). These systems have yet to adjust to the changes in Industry 4.0 which makes them very vulnerable to attacks and also they lack in forensics tools and techniques [1, 6]. Similarly, SCADA systems were originally designed to work in closed networks but with the introduction to IIOT, more and more interconnectivity in its architecture makes it more vulnerable to attacks [10, 11].

Forensics is very important in such systems so as to study attacks and prevent any future attacks [7]. There have been incidents in SCADA systems in recent times like Stuxnet, Translate-Siberian Pipe explosion etc. which have resulted in threat to human life [13, 25]. In this paper we discuss some of the challenges faced in the Digital Forensics in SCADA systems in Industry 4.0 and propose some solutions or directions to explore in order to tackle these problems [32].

This paper is organized as follows. Section II gives an overview of the architecture of SCADA systems. Scenarios of attacks and the need for Digital Forensics are also described in this section. In Section III we discuss the 5-step process for digital forensics. Tools available for forensics are described in Section IV. Challenges in digital forensics in SCADA in Industry 4.0 are highlighted in Section V. Possible solutions are discussed in Section VI and Section VII concludes this paper.

II. INDUSTRIAL CONTROL SYSTEM

Industrial Control System (ICS) is an integration of hardware and software with network connectivity to perform industrial processes. It includes Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controller (PLCs), Remote Terminal Unit (RTU).

A. SCADA Systems:

SCADA systems stand for Supervisory Control and Data Acquisition. It consists of two layers: the control center and the field sites which are connected via the network layer as shown in Fig. 1. The control system consists of HMI (Human Machine Interface), Historian and MTU (Master Terminal Unit). The field sites consist of PLC (Programmable Logic Controller) and RTUs (Remote Terminal Unit). The HMI gives humans the access to control the system and gives a visual representation of the processed data. The MTU is responsible for processing all the data received from the field sites along with providing communication with them. The Historian is used to store all the data, in the form of logs, which is later analyzed. The PLC are connected to the sensors which are responsible for the working of the sensors. The PLCs have a specific programming language which is used to control the functioning of the sensors. It consists of a Central processing unit (CPU), which performs all the data processing, a memory to store the data for processing and a user interface to interact with the data. The RTUs have a similar function as the PLCs. They gather data and transmit it back to the control center. They have a faster CPU and more storage compared to PLCs [4, 34].

B. *Need For Digital Forensics in ICS/SCADA systems:*

The architecture of SCADA is very complex in IIoT. There are multiple access points which increase the chances of cyber-attacks and increase the demand for digital forensics to be performed properly [33]. In SCADA systems, few common types of cyber-attacks are malware, Distributed denial of service (DDoS), worm, bots, resilience, privacy and intrusion detection attacks. In recent years we have seen incidents like Stuxnet, which is a malicious worm, which was introduced in Iran's nuclear facilities. It traveled through the USB sticks and affected the functioning of PLC by updating its code. It damaged the centrifuges which were essential for uranium enrichment. Another such accident that took place was the Trans-Siberian Pipe explosion where a Trojan horse was introduced in the SCADA system that ran the pipeline. The Trojan horse changed the pump speed and the valve settings causing it to explode [16].Seeing such cases increases the demand for digital forensics to work properly and to make sure such accidents do not take place again in the future.

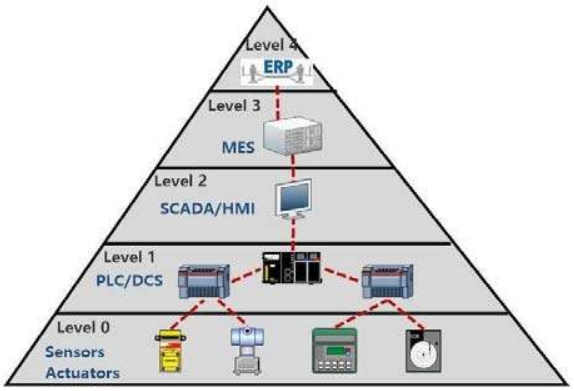

Fig. 1. SCADA Architecture [35].

III. DIGITAL FORENSICS IN SCADA SYSTEMS

The process of forensics in SCADA systems takes place in 5 steps as shown in Fig. 2.

A. *Examination*

This step includes understanding all sources of evidence from all sources in the SCADA system which can be internal or external systems. In this step, the network diagrams, configuration details, logs and credentials are obtained [28].

B. *Identification*

This step involves identifying the operating system of the PLCs, network designs and implementations. Next the tools are identified for the forensic process. It makes use of the information obtained from the Examination stage and identifies all the requirements for the forensic process [29].

C. *Collection*

This step involves collecting all the data which is identified in the previous steps. It involves collecting network traffic, volatile and non-volatile memory and all sorts of information. The captured data is captured in external devices so as to be more secure and safe. Forensics tools like Wireshark, Network Miner, Encase, TCPDump, and FTK Imager are used.

D. *Analysis*

In this step the collected evidence is analyzed and a timeline of all the activities leading up to the attack is created and analyzed. The deleted data is restored in this stage. Forensics tools such as Autopsy, Volatility, Encase, FTK Imager, Wireshark are used [20, 23].

E. *Documentation*

In order to prevent tampering of the data, a proper detailed documentation needs to be done of the date, time, person and other information [26]. After this step all the results are reported to individuals who include the person commissioning the investigation or the employing company and this report is used as evidence in court.

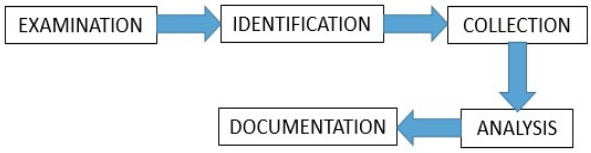

Fig. 2. Digital Forensics Process.

IV. FORENSICS TOOLS AVAILABLE

A. *Autopsy Sleuth Kit*

The autopsy sleuth kit is a very important forensics tool which allows users to analyze hard drives and recover data/files from it. These hard drives are the exact copy of the affected drives which is done during the process of acquisition for forensics. It is an easy to use and fast processing digital forensics platform [2, 3].

B. *Wireshark*

Wireshark tool is used to capture the network traffic and the packets of data being transferred on the networks like Ethernet, Bluetooth, wireless. It gives us information about what all is going on the network which helps for analysis in forensics [8, 9].

C. *Network Miner*

Network Miners capture packets to detect hostnames, sessions, open ports and operating systems without generating traffic on the network. It saves time for forensic analysts by presenting extracted data with a user-friendly interface. It works on an Operating system (OS), which is a system software providing an interface between user and hardware, like Windows, Linux, and UNIX.

D. *Encase*

Encase forensic tool is used for data acquisition and data analysis. It acquires evidence from the data obtained from the HMI and can be used to perform the in depth analysis. It has many inbuilt data processing features. It works on Windows operating systems [12].

E. *Volatility*

Volatility is a forensic tool which is used for performing malware analysis. It is an open source python base program

and can be used for O.S. like Windows, Linux, Mac and Android. For SCADA it can be used to perform live data processing on acquired data from HMI and communication centers.

F. FTK Imager

Similar to Encase, FTK Imager is used for data acquisition from Windows operating systems and is used for data analysis. It issued to process the evidence/data acquired from HMI and communication centers.

G. TCPDump

It is similar to Wireshark and Network miner, is used to acquire network traffic from the communication region. It dumps all the network traffic post the attack for forensics analysis [17, 30].

V. Challenges In SCADA Forensics

A. Lack of post forensics models and tools.

The SCADA system compared to IT infrastructures is different. It consists of 2 layers- the control center and the field sites. The control center consists of HMI (Human Machine Interface) and MTI (Master Terminal Interface). The field sites consist of PLC (Programmable Logic Controller) and RTU (Remote Terminal Unit). This makes the architecture more complicated [15]. In case of an attack, the big and complicated architecture requires well developed forensics models and tools to be able to successfully identify the attack and acquire the data. Most current digital forensic tools are designed to run on a single workstation, with the investigator issuing queries against copies of the acquired data evidence. With current generation tools, the single workstation model works reasonably well and allows tolerable case turnaround times for small forensic targets. They are unable to work properly on large targets which includes networked systems (SCADA). The problem we face in SCADA systems is that it is a live system and because of the volatile memory, the state of the machine is recorded in the volatile memory which keeps on changing, it's tough to acquire data. So once the attack happens, to perform post forensics, the tools available right now would not be able to acquire the whole evidence as some of the evidence would be lost while shutting down the system

B. Lacks live forensics

SCADA systems are live all the time. The control center transmits data to the field sites which perform the tasks and keep transmitting data back to the control center. It has two types of memory, volatile and non-volatile memory. The non-volatile is stored in hard disks which contain a lot of storage. The volatile memory, which contains the state of the system, is very important for digital forensics in case of an attack. But the problem is as the storage is limited, the volatile memory resets and we are unable to get the lost state of the machine. Therefore due to the unavailability of post forensics tools and models, live forensics is very important to be able to respond immediately in case of an attack. Current live forensics tools are set up for operating systems like Windows or UNIX but in case of the SCADA systems, the embedded devices having a different operating system, are not compatible with the current live forensics tools [5].

C. Lack of ground truth for forensics data as data can be tampered during communication

With the introduction of Industry 4.0, everything works on networks. In SCADA systems, the data is transferred from control center to field sites and vice versa via networks using internal networks or the internet. This data, during the communication stage, can be tampered with. This would result in false information or insufficient information while performing forensics. There are a few tools to monitor the networks but they are not up to the mark. Like the Wireshark tool which gets the packets of data from the network for forensics but it has its cons as it cannot be used to perform more tasks like analysis or determining an attack. It just gives all the information in which most of it is irrelevant information. Therefore there is a lack of ground truth for forensics data [22].

D. Volatile memory and limited logging so data retrieval is tough

SCADA systems are online most of the time and consist of volatile and non-volatile memory. The volatile memory stores the logs i.e. the state of the machine and its capacity is very low. The non-volatile memory is stored in large hard drives. Due to the limited volatile memory, the older logs and state of the machine gets removed. This causes the loss of vital information for digital forensics as the state of the machine is very important for the same [24, 31].

E. Challenges in Forensics Tools

The forensics tools currently available for SCADA face a lot of challenges. Tools like Autopsy, Encase, and FTK Imager work only on specific operating systems like UNIX, Windows, and Mac. But SCADA's field devices (PLCs and RTUs) have completely different operating systems so these tools would not function properly. These tools work on the HMI but during an attack, the data transferred from PLCs and RTUs to HMI can be manipulated and changed and so the data to be analyzed with these tools would not be correct. And tools like Volatility which can be used to perform live forensics faces the same issue as it can only work on Windows operating systems. Tools like TCPDump, Wireshark and Network Miner captures data from the network (the communication center) and then transfers for analysis but while doing so the data can be tampered and evidence could be lost. Also it sends all the network traffic information which contains relevant and mostly irrelevant data for the forensics and it would take up a lot of time to go through all this data and get to the relevant part.

VI. Possible Solutions That Can Be Developed

The following proposed solutions tackle a few of the forensics problems like the problem of lack of live forensics, lack of digital forensics tools, volatile memory issues and the shortcomings in Wireshark tool.

A. Interrupt Raising Model

One solution for live forensics is creating a Model which raises an interrupt whenever there is an anomaly. The Model would be taught types of anomalies and would detect the anomaly and would raise an interrupt. The interrupt would result in storing of the logs (state) of the machine which will later be used for forensic processes [10].

B. *Model Integrated with Wireshark to detect network anomaly*

Wireshark lacks the ability to determine in case of an attack and also it will send data of all the things going on in the network which would be useless and would take a lot of time to analyze before finally getting to the important part. So integrating it with a model which would be trained with network anomaly data would help to determine in case of a network attack [1].

C. *Tools for PLC*

The operating system of PLC is completely different compared to that of IT systems. It has a local OS. The current forensics tools are unable to run on the PLCs OS. So compatible forensic tools are required for PLC's operating system [15].

D. *Expanding the Volatile Memory/ Using cloud services*

The volatile memory of the SCADA system keeps the logs of the state of the machine which is important for forensics. The memory is very small and keeps on refreshing so expanding the memory or making use of cloud services could solve this issue [14].

VII. CHALLENGES ARISING WITH SOLUTIONS

A. *PLC/RTU Architecture and Malware Parameter*

Proper understanding of the PLC/RTU architecture and the parameters of a malware are required to implement the Interrupt Raising Model.

B. *Wireshark Challenges*

To perform deep packet inspection, parameters of the Operational Technology (OT) packets, which are basically data communication within the physical system, are required to determine in case of a malicious attack.

C. *Memory Expansion Problem*

For using Cloud Services to expand the volatile memory, it would be costly as there are multiple PLCs and RTUs being used in a SCADA system and expanding each of them would be costly.

D. *Lack of Standardization*

Lack of standardization for machine to machine data exchange and architecture for processing continues to be challenging and it is detrimental to innovation and creation of Intellectual Property.

VIII. CONCLUSION

Industry 4.0 or the IIoT has increased the connectivity, automation and real time data processing. It has introduced terms like Artificial Intelligence, Internet of Things, Big Data,etc. in industry processes. However, with the increase in connectivity, there is also an increase in cyber-crimes especially in systems like SCADA. In this paper, we discuss the digital forensics challenges faced by SCADA systems. The architecture of SCADA systems being different from other IT systems, has made it vulnerable and not compatible with current digital forensics methods/tools/models. We have identified and compiled some major shortcomings in them such as: lack of post forensics tools and models, lack of live forensic tools, lack of ground truth for forensic data as the network can be tampered with, and limited logging capacity due to having a volatile memory. We also propose some solutions to tackle these identified problems. The lack of live forensics would be solved by creating a model which raises an interrupt in case of an attack. Another model which would be integrated with Wireshark tool may be employed to detect network anomalies, and forensic tools can be specifically created for PLCs OS. Further, the issue of limited logging can be solved by expanding the volatile memory to increase the logging capacity. These directions need to be explored further and solutions need to be found for successful forensics in SCADA systems of Industry 4.0.

REFERENCES

[1] T. Kilpatrick, J. González, R. Chandia, M. Papa and S. Shenoi, "An architecture for SCADA network forensics", in Advances in Digital Forensics II - IFIP International Conference on Digital Forensics, National Centre for Forensic Science, Orlando, Florida, USA, 2006.

[2] S. Yadav, K. Ahmad and J. Shekhar, "Analysis of Digital Forensic Tools and Investigation Process", in High Performance Architecture and Grid Computing - International Conference, Chandigarh, India, 2011.

[3] S. Raghavan and S. Raghavan, "A study of Forensic and Analysis Tools", in Eighth International Conference on Systematic Approaches to Digital Forensic Engineering, Hong Kong, China, 2013.

[4] T. Wu, J. Pagna Diss, K. Jones and A. Campos, "Towards a SCADA Forensics Architecture", in 1st International Symposium for ICS and SCADA Cyber Security Research, 2013.

[5] P. Taveras, "SCADA LIVE FORENSICS: REAL TIME DATA ACQUISITION PROCESS TO DETECT, PREVENT OR EVALUATE CRITICAL SITUATIONS", in 1st Annual International Interdisciplinary Conference, Azores, Portugal, 2013.

[6] J. Stirland, K. Jones, H. Janicke and T. Wu, "Developing Cyber Forensics for SCADA Industrial Control Systems", in The International Conference on Information Security and Cyber Forensics, Universiti Sultan Zainal Abidin (UniSZA), Kuala Terengganu, Malaysia, 2014.

[7] P. Eden, P. Burnap, A. Blyth, K. Jones, H. Soulsby and Y. CHERDANTSEVA, "A Forensic Taxonomy of SCADA Systems and Approach to Incident Response", in 3rd International Symposium for ICS and SCADA Cyber Security Research, 2015.

[8] A. Venčkauskas, J. Toldinas, S. Grigaliunas, R. Damasevicius and V. Jusas, "Suitability of the digital forensic tools for investigation of cybercrime in the Internet of Things and Services" in RCITD, 2015.

[9] N. Loja, R. Morocho and J. Novillo, "Digital Forensics Tools", in International Journal of Applied Engineering Research, 2016.

[10] P. Vliet, T. Kechadi and N. Le-Khac, "Forensics in Industrial Control System: A Case Study", in Conference on Cyber security of Industrial Control Systems Workshop on the Security of Cyber Physical Systems, 2016.

[11] D. Vuksanović, J. Vešić and D. Korčok, "Industry 4.0: the Future Concepts and New Visions of Factory of the Future Development", in Sinteza, 2016.

[12] K. Ghazinour, D. Vakharia, K. Kannaji and R. Satyakumar, "A study on digital forensic tools", in IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), 2017.

[13] P. Eden, A. Blyth, K. Jones, H. Soulsby, P. Burnap, Y. CHERDANTSEVA and K. Stoddart, "SCADA System Forensic Analysis Within IIoT", in Cyber security for Industry 4.0 (pp.73-101), 2017.

[14] L. Caviglione, S. Wendzel and W. Mazurczyk, "The Future of Digital Forensics: Challenges and the Road Ahead", in IEEE Security and Privacy Magazine. IEEE Security and Privacy Magazine 15(6). 2017.

[15] R.L. Awad, S.A. Beztchi, J.M. Smith, J.B. Lyles and S.J. Prowell, "Tools, Techniques, and Methodologies: A Survey of Digital Forensics for SCADA Systems", in The 4th Annual Industrial Control System Security Workshop, 2018.

[16] L. Luciano, I. Baggili, M. Topor, P. Casey and F. Breitinger, "Digital Forensics in the Next Five Years", in The 13th International Conference, 2018.

[17] M. Al-Sadi, L. Chen and R. Haddad, "Internet of Things Digital Forensic Investigation Using Open Source Gears", in Southeast Con, 2018.

[18] S. Vaidya, P. Ambad and S. Bhosle, “Industry 4.0 – A Glimpse”, in Procedia Manufacturing 20:233-238. 2018.
[19] S. Kumar, B. Narkhede and K. Jain, “Industry 4.0: Literature Review and Future Research Directions”, in Rotre of Industrial Engin. in Industry 4.0 Paradigm, Bhubaneswar, Odisha, India, 2018.
[20] U. Karabiyik, N. Celebi, F. Yildiz, J. Holekamp and K. Rabeh, “Forensic Analysis of SCADA/ICS System with Security and Vulnerability Assessment”, in ASEE Annual Conference and Exposition, 2018.
[21] S. Sathwara, N. Dutta and E. Pricop, “IoT Forensic -- A digital investigation framework for IoT systems”, 2019.
[22] S. Ghosh and S. Sampalli, “A Survey of Security in SCADA Networks: Current Issues and Future Challenges”, in IEEE Access PP(99):1-1, 2019.
[23] H. Villar-Vega, L. Perez-Lopez and J. Moreno-Sanchez, “Computer forensic analysis protocols review focused on digital evidence recovery in hard disks devices”, in Journal of Physics Conference Series 1418:012008, 2019.
[24] A. Iqbal, F. Mahmood and M. Ekstedt, “Digital Forensic Analysis of Industrial Control Systems Using Sandboxing: A Case of WAMPAC Applications in the Power Systems” in Energies 12(13):2598, 2019.
[25] E. Ateş, G.E. Bostanci and M. Guzel, “Security Evaluation of Industry 4.0: Understanding Industry 4.0 on the Basis of Crime, Big Data, Internet of Things (IoT) and Cyber Physical Systems”, 2020.
[26] N. Mohamed, J. Al-Jaroodi and I. Jawhar, “Cyber–Physical Systems Forensics: Today and Tomorrow”, in Journal of Sensor and Actuator Networks, 2020.
[27] O. Bongomin, G. G. Ocen, E. O. Nganyi, A. Musinguzi and T. Omara, “Exponential Disruptive Technologies and the Required Skills of Industry 4.0”, in Journal of Engineering 2020:1-17, 2020.
[28] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. Markakis, “A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues”, in IEEE Communications Surveys and Tutorials PP(99):1-1, 2020.
[29] S. Sharma, K. Ghanshala and S. Mohan, “Advanced Digital Forensic IoT Based Secure Communication”, 2020.
[30] S. Sachdeva, B. Raina and A. Sharma, “Analysis of Digital Forensic Tools”, in Journal of Computational and Theoretical Nanoscience.17 (6):2459-2467, 2020.
[31] B.R. Yogeshwar, M. Sethumadhavan, S. Srinivasan, P.P. Amritha, “A Light-Weight Cyber Security Implementation for Industrial SCADA Systems in the Industries 4.0”, in Information and Communication Technology for Intelligent Systems (pp.463-472), 2021.
[32] S. Mrdovic, “IoT Forensics”, in Security of Ubiquitous Computing Systems (pp.215-229), 2021.
[33] G. Yadav and K. Paul, “Architecture and security of SCADA systems: A review”, in International Journal of Critical Infrastructure Protection. 34(Sgc):100433, 2021.
[34] C. Jayathilaka, “A Literature Review of Cryptographic solutions used in SCADA to ensure its security”, 2021.
[35] W. Dai, P. Wang, W. Sun, X. Wu, H. Zhang, V. Vyatkin and G. Yang, “Semantic Integration of Plug-and-Play Software Components for Industrial Edges Based on Micro services”, PP(99):1-1, 2019.