International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Industrial Internet of Things (IIoT) of Forensic and Vulnerabilities

Venkata Venugopal Rao Gudlur, Vikneswara Abirama Shanmugan, Sundresan Perumal, Radin Maya Saphira Radin Mohammed

Abstract: ***The Industrial Internet-of-Things (IIoT) have changed the present world and future technology-based Industry 4.0, however the understanding of Industrial Internet of things (IIoT) has turned out to be big challenge as far as security concern. The main purpose of adopting and going with new technologies will bring new challenges with cybersecurity and will have more expose uncertain vulnerabilities in terms of AI and BI applications and usage with forensic investigation and accuracy of information sharing between smart devices. This paper composed on the utilization of Artificial Intelligence in securing required evidence for forensic investigation process. The legal methods are different as per region and industry, but the back-frame work and case-based thinking are similar. This framework is made from Intelligence systems such as AI and BI too dependent on the digital information from cloud server. The information from Business Intelligence (BI) and Artificial Intelligence (AI) intersects with data on cloud-based server requires more secure network process and firewall to prevent cyber intruders. This paper has discovered a few gaps on security issues and vulnerabilities where as it will cater proper IIoT based procedure for the Digital Forensic Investigation process.***

Keywords: Artificial Intelligence (AI), Business Intelligence (BI), Digital Forensic Investigation (DFI), Industrial Internet of things (IIoT).

I. INTRODUCTION

The IIoT security is not a one-time investment when it comes to industry 4.0. Every utility and critical infrastructure needs to consider each device that has communication process for smooth and smart operations in technological filed. Digitalized secure networks ply an important role to process a better methodology and connectivity for best outcome for Industry 4.0. It starts with technical flow and better communication capabilities between intelligent systems such as AI and BI. The encrypting and authenticating the data using private networks are biggest challenge for secure process flow [1]. Whereas the secure process flow has been designed to protect IIoT based communication system and connection where data is being collected and delivered.

Today, more advanced sensors are being developed with more secure integration with smart tools along with AI and BI to monitor cyber intruders. The digital security must advance and envision progressively complex and inventive assaults. There are currently over 13 billion connected smart devices operating in the field of IIoT and Industry 4.0 and each device likely has at least one loophole or backdoor that could serve as an entry into or access critical infrastructure data from cloud server [2]. Therefore, we have a focusing the more on smart devices with more secure connected to future industry and smart devises like IIoT. The smart technology related to cyber security and best practices and procedures has to enhance implementation capabilities when it comes to secure personnel and financial data. The current data analysts are predicted around 40.5 billion insecure smart (IoT based) devices are developed and connected in the field by the 2025 and it may increase the number for fast growing need industry 4.0.

II. LITERATURE REVIEW

The condemnatory to development of a multi-layered and multi-dimensional cyber security related solution that reduce the risk some extent to the IIoT and helps to DFI. The IIoT devises that deliver data to cloud server need a proper network pathway that is secure and hard to intercept by intruders. These devices should use by a fixed IP address and secure system when they require for more secure network process. The devices are requiring authentication process to protect the server with proper intrusion detection and prevention methods to safe guard from cyber intruders. The dynamic IP locations for the information sessions to the safe framework just when required [3] [4]. Confirmation is important step to safeguard network; it ensures that unidentified devices can't intrude with network for correspondence. An extra dimension of security is confining the gadget's correspondence to short interims and when the information transmission is finished, the gadget stops the correspondence channel.

Manuscript received on January 02, 2020.
Revised Manuscript received on January 15, 2020.
Manuscript published on January 30, 2020.
* Correspondence Author
Venkata Venugopal Rao Gudlur *, Center for Post Graduate Studies, Limkokwing University of Creative Technology, Cyberjaya, Malaysia.
Vikneswara Abirama Shanmugan, Department of Water and Environmental Engineering, Universiti Tun Hussein Onn Malaysia, Batu Pahat, Malaysia.
Sundresan Perumal, Faculty of Science & Technology, Universiti Sains Islam Malaysia (USIM) Nilai, Malaysia.
Radin Maya Saphira Radin Mohammed, Department of Water and Environmental Engineering, Universiti Tun Hussein Onn Malaysia, Batu Pahat, Malaysia.

Programmers are ready to connect and configure devices with proper firewall with effective verification, and unravel the encryption, which is hard to accomplish.The cloud based data storage is one of the most common method in the digital marketing and consumer industry today but has some difficulties when it comes to data security and data storage. The digitalized industry end users prefer to bypass third-party tools and cloud based storage facilities with more data security and data delivery through smart devices to their closed secure networks or secure third-party systems. The entire process can only be achieved by investing in smart and cyber security with checking more on less vulnerable seamless system integrated end-users systems for cloud computing and data storage [5] [6]. Supply Chain and ID 4.0 will have future unpredictability in terms of the secure cloud based storage and considering the future predictive damage that could result and effect on the digital data was accessed by intruder to further damage. Most of the smart industry related companies are offering the utmost secure digital data transmission protocol connected to secure servers in addition to cloud based storage. Sometimes possibility; they may follow very poor-quality unsecured or unstructured network protocol or process.

A. Related Work

There are many different approaches and process have been proposed to deal with the three aspects presented in this paper, to minimize the amount of digital evidences process or examined, and correlation of digital evidences and distribution of digital forensic examinations with more computational work has to be finalized. There are various types of smart devices that communicates with a secure system to create an entry point into the cloud based server. The most infamous example of a digital vulnerability and attacking to a secure system connected to a smart devises was a malicious virus known as Stuxnet which can harm extensively to the digital data and even entire network system [7] [8]. The viruses has been took over Iranian uranium enrichment plant for over a year without being detected by the experts and computerized tools and protected devices. The Stuxnet system has been manipulated the digital data and system and with more damaged the centralized systems with clear data structure as well as the enrichment process. It has been believed that attack was carried out via infected USB drives which is not been investigated properly and clearly demonstrating the vulnerability of the current network system. After the attack many of the industries and organizations started to worry about their own censorious infrastructure with implementation of cyber security and digital forensic task forces to regulate security and process with regulated requirements [9] [10].

The most of the IIoT companies has their own security issues that will be the next step securing the digital data. This can be illustrated by example, in a milk treatment plant, where cyber intruders could inject false preservatives when they do data readings and then feed the false digital data to the secure system through various means using digital equipment's and tools. But sometimes it is not possible to detect the tampered digital data, which is very critical and most of the infrastructure operators need to implement preventative security measures as part of their standard operating procedures [11] [12]. There are few useful software tools to prevent false data injection by intruder in to an automated system or network to detect suspicious activity which they can deploy or integrate with their current network. This can be elaborate with a simple example, when monitoring milk, if the cholesterol and calcium level spikes, the purity of milk are likely to drop and cannot be preserved the date specified by system and it will show wrong information. There are some machine learning algorithms which is called AI can automatically link and learn such relationships between various parameters within and warn if one parameter deviates from another and its expected behavior and will updated to the current process flow [13].

III. IIOT AND INDUSTRY 4.0

The Digitization of an Industry 4.0, which will be quicker and updated methodologies of item appropriation decrease the conveyance time of high sprinters to couple of hours with accurate information sharing and storing in to the secure database. The reason for these administrations is worked by cutting edge with advanced approaches, e.g., prescient investigation of inside (e.g., request) and outside (e.g., advertise patterns, climate, financial data, information stored at could and other files) information and in addition machine status information with sensors connectivity to smart gadgets, and gives a significantly more exact results as per client request [14] [15]. Things are not completed on a month to month premise, but rather week by week, and for the plain quick moving items even each day when it comes to smart supply chain industry. Later, we will see "prescient delivery," for which Amazon holds a patent - items are dispatched before the client submits a request and process will be done. The client arrangement is later coordinated with shipment that is now in the coordinated to organize with the help of smart devices (being transported towards the client district) and the shipment is rerouted to the correct client goal more adaptable and accurate [16].

A. IIoT Best Practices with BI and AI

Cyber security and Venerability are not a one-time investment for IIoT related Industry 4.0. The technological advanced and with a more complex infrastructure related to operator needs to consider every smart device that has a communication capability to protect customized solutions designed for industry 4.0. Every smart component in the internal network when identifies the devices with IIoT sensors for better and clear communication capabilities will supply external or internal smart device vendors and required to check the network vulnerabilities for more safe and secure digital data flow and quick analysis [17]. Current researches are discovering how to implement the best practices in the IIoT industry with more secure data storage and access capabilities using a private secure network by secure BI and AI tools in the field of deployed devices at machines. Sometime the longer process of authentication is minimizing the usage of the smart devices without a proper communication channel, with more restricted communication between the smart devices and the machines.

The smart security features should be designed such a way to protect the digitalized smart systems with connecting point where digital data is being transferred or collected and transferred to the frontend users. As of today, the more technological and advancement in IIoT sensors are being connected and integrated with software and mobile based tools and applications. These devices where as DFI process to collect the evidence is bit easier for secure environment [18] [19].

Table- I: Comparison Forensic Models with Proposed Model

IIoT Digital Forensic Model and Comparison	IIoT Devices	Monitoring Phase	Abnormal Activity	Secure Location / IDS/IPS	Base Device Identification	Examination	Evidence Analysis	Results	Proof of Defence	Documentation	Storage
Venkata Venugopal (Current Study)	●	●	●	●	●	●	●	●	●	●	●
K.Kyei et al		●			●	●	●	●	●	●	●
A.Agawal el al				●	●	●	●	●	●	●	
I.O Ademu el al					●	●	●	●		●	●
V.Baryamureeba and F.Tushabe		●	●	●	●	●	●	●		●	●
B.Carrier and E.H Spafford				●	●		●	●		●	●

There are currently over 16 billion connected devices with BI and AI integrated with could server. Systems in the field are connected to smart devices likely to have an at least one loophole or backdoor that could serve as an entry point to an intruder in any sophisticated secure infrastructure and digital data. The entire press need to secure all with smart devices before we continue to take over the current technology market with more additional IIoT devices for better industry needs [20]. The advanced cyber security best practices and DFI need to be implemented time to time when it comes to technology upgrade and digital industrialization. Therefor we can reach a point of no return, with the predicted 40.5 billion insecure IoT devices deployed in the field for future technological changes in in the industry 4.0.

B. Proposed IIoT DFT Model and Technical Process

Tools used in proposed IIoT Security Forensic Process are also trained with similar solved cases earlier with formal forensic investigation process. Such as: Monitoring, AI and BI tools will be having data from cloud server as a proof of defence. As mentioned in above proposed flow the smart analysis is considered here as a part of complete AI /BI based framework with IIoT and as a separate process and this model is only proposed requires more detailed study to make it more suitable for other industries globally. The AI algorithms can be more supportive when argumentation and narrative based communication will takes place with more statistical evidence with internal or external building justice on AI developed models of argumentation and future scenario construction for better results.

The AI will have the real time show events in a graphical structures that can be used to express scenarios based and support probabilistic reasoning for future analytics. But the AI can also give modelled scenario which will be more useful for augmenting in terms of decision making by lawyers and judgment from the judges in judicial court [21]. The most of the cases AI helps in different format and structurally to the judges can evaluate with more realistic informative data for the better judgment. The AI can do real time meta-analysis or analytics for the Meta knowledge that is available from different sources which can be simplified with the complex data into an understandable language that can be translated within a short period of time. When AI can provide more create repository that would contain the known well sanitized with more relevant examples on digital forensic investigations with more information on known properties and results for the investigators which is more reliable and up-to-date.

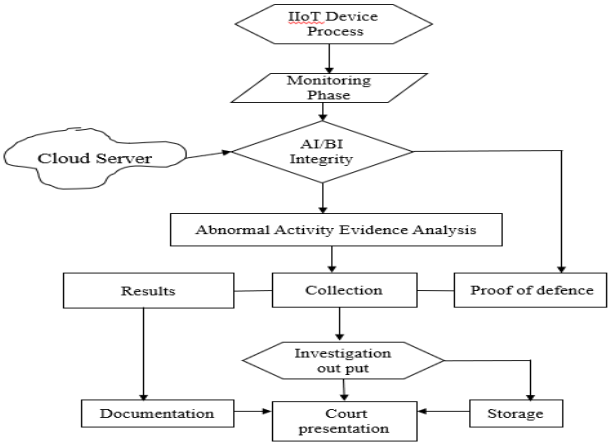

Fig. 1.Proposed IIoT security forensic process flow.

IV. PROPOSED ARCHITECTURE

This section explains about the possibilities how to apply AI to digital forensics are identified with the more focused and disciplined manner. The examining the ways in which the application of AI can enhanced with in digital forensics investigations process. The main discovery in this paper is to enter the debate as such what constitutes AI and digital forensic data or investigation and except to say that within the context of this paper AI is taken to a system that is connected to various devices and models are have some degree of intelligence such as smart devices or connectivity with IIoT and modern machines and technology [22]. The entire application and process of intelligence system with in computer and digital forensics investigations takes on several components. At same time or various stages of the investigation in life cycle of digital forensic investigation process flow and regards to acquiring digital evidence, the analysis of acquired digital evidence and the presentation of that evidence followed by preservation.

The entire process each of these stages the basic skill and knowledge of the digital forensic tools and process flow for an investigator is a fundamental to the success of any investigation.

A. Limitations

Major limitation of this framework is its dependency on training data sets.

If there is a case which is reported first time then this framework may not be able to handle it, however as discussed in previous section all the three smart technologies can work with AI and non-AI conditions. Another limitation is size of training data sets, a huge amount of data is required to train this system to make it more accurate and powerful. It may seem difficult from the forensic investigator's point of view to train the system with large amount of data covering majority of common cases, but it is equally easy for the manufacturers [23].

Training is crucial step of this proposed framework and can assure reliability of the work done by such system.

The other limitation could be uncommon cases; however, this framework can be trained from regularly reported crimes like malware infection, document forgery, unauthorized access, etc. but it may not be trained for cases which are committed occasionally. Though such cases are very rare, they are important and can be solved with traditional way of non-AI component of the proposed framework. Final limitation observed at this stage is authenticity of the reports generated by the smart system. However, thorough training will reduce false positives, the investigator is required to verify and cross check the finding of the proposed framework before submitting it in the court of law [24]

V. CONCLUSION

The distributed platform AI and BI are presented promising results in terms of IIoT which indicate that the system can sustain more machines with sensor technology then before for proper basic communication between the humans and smart machines for better results. This various connected devices in nature allows us to conceive new data analysis that are very expensive in terms of acquiring latest computer resources and tools. The knowledge management and could not be carried by a single tools or network device or secure firewall to protect from intruders from time to time. The forensic investigation process on these devices can be taken as challenge for modern forensic investigators but should get the results with in idle time of the computer available in the forensic laboratory [25].

The current forensic team can look in to implementation techniques and third party operators that perform time-consuming data analysis such as bio matric face recognition or keyword search in a distributed systems that connected to network. The more often users will try to do with password breaking software and secure tools to collect the digital evidence. The combination of AI and BI integration with IIoT will reduce in the risk of vulnerabilities but cannot agree with zero error and possibility of attacks by cyber criminals [26]. The volume of evidences to be examined by the expert and they collect from these smart devices will arise question on authenticity and data collected from the stored location for further examination. The possibility of technical and mechanical errors from these devices which cannot be avoided. This should lead biggest challenge for digital forensic investigators that face more challenges in terms of keep changing technological advancement and digitalization around the globe with volume of digital evidence.

ACKNOWLEDGMENT

I would like to thanks to my co-author Vikneswara Abirama Shanmugan sharing knowledge to publish this paper and my supervisor who always encourages with technical knowledge.

REFERENCES

1. 2016: Current State of Cybercrime, RSA Whitepaper
2. World Internet Users and 2017 Population Stats, 10th July, 2017 [http://http://www.internetworldstats.com/stats.htm]
3. “IoT’ connected smart devices.” Juniper Research, 28 July 2015. Web. Retrieved 8 Mar. 2016.
4. FBI, IC3. ICCC (IC3) 2015. Web. Retrieved 10 March 2016. http://www.ic3.gov/media/2015/150623.aspx
5. “SCADA vulnerability on the rise - EETimes. Rich Quinnell, 24 Sept. 2015. Web. 26 Apr. 2016. Id=1327785
6. Kushner, David. The real story of stuxnet.” IEEE Spectrum. 2016.
7. Morgan, Steven C. “Cyber Security Market Report.” 2016.
8. Zawoad, S. & Hasan, R., 2015. FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. - 2015 IEEE International Conference on Services Computing, SCC 2015. pp. 279–284.
9. Charlie Osborne, 2016. Insulin pump vulnerabilities could lead to overdose (2016).
10. Borgohain, T., Kumar, U. & Sanyal, S., 2015. Survey of Security and Privacy Issues of Internet of Things.
11. Huuck, R., 2015. IoT: The Internet of Threats and Static Program Analysis Defense.
12. IBM. I2 Intelligence Analysis Platform. Available online: http://www-03.ibm.com/software/products/en/intelligence-analysis-platform (accessed on 4 July 2019).
13. Federal Bureau of Investigation (FBI). 2013, Piecing Together Digital Evidence
14. Bradley, J., Barbier, J., Handler, D., "Embracing the internet of everything to capture your share of $14.4 trillion-2013.
15. Oriwoh, E. et al., 2013. Internet of Things Forensics:Challenges and Approaches., pp.608–615. Available at: http://eudl.eu/doi/10.4108/icst.collaboratecom.2013.25 4159.
16. J. Gantz and D. Reinsel. THE DIGITAL UNIVERSE IN 2020: Big data, bigger digital shadows, and biggest growth in the Far East. http://www.emc.com/collateral/analystreports/idc-the-digital-universe-in-2020.pdf.
17. L. Coetzee and G. Olivrin, "Inclusion through the Internet of Things," Assistive Technologies, Fernando Auat Cheein (Ed.), ISBN, pp. 978-953, 2012
18. Induruwa, "Hidden in the clouds: The impact on data security and forensic investigation, 2011, pp. 77-77.
19. Y. Yusoff, R. Ismail and Z. Hassan, "Common Phases of Computer Forensics Investigation Models,” vol. 3, 2011.
20. U.S. Department of Justice, Regional Computer Forensics Laboratory (RCFL). Virginia, Maryland, USA, 2011.
21. Grispos, G.; Storer, T.; Glisson, W.B. Calm before the storm: the challenges of cloud computing in digital forensics. 2012.
22. EURIM-ippr. (2004). EURIM—IPPR E-Crime Study: Partnership Policing for the Information Society. (Accessed on 31 December 2018).
23. Garfinkel, S.L., 2010. Digital forensics research: The next 10 years. Digital Investigation.
24. Luger GF (2010) AI: structures and strategies for complex problem solving. Russell S, Norvig P (Eds.), USA.
25. Duce DA, Mitchell FR, Turner P (2007) Digital forensics: challenges and opportunities.
26. Simson L. Gar¯nkel. Forensic feature extraction and cross-drive analysis. Digital Investigation, 2006.

AUTHORS PROFILE

Venkata Venugopal Rao Gudlur (Phd) Aspirant. IoT Based Digital Forensic Investigation Process, Chartered Member of the Chartered Institute of Logistics and Transport Malaysia, Working as a Head of School Digital Transformation and Sr.IT Lecturer.

Vikneswara Abirama Shanmugan, M. Eng. (Hons.) Civil Engineering Currently pursuing PhD in Civil Engineering at Universiti Tun Hussein Onn Malaysia. Working as a lecturer for past 2 years and has worked as a civil engineer for 2 years before that. Publications and research carried out mainly focusses on the field of water and environmental engineering, green technology and Industrial Internet of Things (IIoT)