Global Scientific JOURNALS
GSJ: Volume 10, Issue 9, September 2022, Online: ISSN 2320-9186
www.globalscientificjournal.com

Review paper to enhance authentication of IoT devices in Industrial Control Systems

Jahid Hasan Miah
Student IT Department
Tshwane University of Technology
Soshanguve, South Africa
antormiah@protonmail.com

Tonderai Muchenje
Lecturer IT Department
Tshwane University of Technology
Soshanguve, South Africa
muchenjet@tut.ac.za

***Abstract*—Industrial Control Systems are hardware and particular manipulating structures used to automate and modify diverse industrial operations and procedures. ICS incorporates devices, networks, and configurations applied to operate and optimise more than one strategy withinside the manufacturing chain. However, this layout no longer meets trendy commercial enterprise necessities for working with cutting-edge technologies like big data analytics. Therefore, to meet the industry requirements, various ICSs had been linked to agency networks that permit commercial organisation customers to get the right of entry to real-time statistics generated using power plants. Which led to the extinction of the air gap in ICS; thus, many ICS security challenges arose. This paper reviewed cyber security issues related to ICS and decided to solve one specific problem. Weak authentication of IoT devices in ICS is the only problem proposed to be solved in this research by implementing an algorithm using the MATLAB simulator to enhance the authentication of IoT devices in ICS.**

***Keywords*—Industrial Control Systems (ICS), Internet of Things (IoT), Programmable Logic Controller (PLC), Distributed Control System (DCS).**

I. Introduction

Industrial Control Systems are used for dealing with, directing, and regulating the behaviour of automated industrial strategies. ICS is a period that encompasses numerous types of control systems, but all these systems have a few simple developments in the commonplace. Their task is to supply a preferred result, typically retaining a target country or to perform a positive assignment in commercial surroundings. They perform these operations using sensors and actuators to acquire real-global records. They then compare this information with preferred set points and compute and execute command features to control tactics via final manipulate elements, including managing valves, to keep desired states or complete duties.

Recent trends in ICS' cybersecurity surveyed by The State of Industrial Cybersecurity by Kaspersky are and Claroty: Due to covid 19, most companies decided to work remotely. Around 70 per cent of ICS organisations reported increased vulnerabilities. Increased remote work increased remote cyber-attacks on ICS. Moreover, weakness in PLCs increased by 28.9%. However, engineering workstations are worse, rising to 57.7%. Also, In the first half of 2019, attacks increased by 122.1% in the water and sewage sectors, growing by 87.3% and 58.9% in the critical manufacturing and energy sectors, respectively.

Lastly, when asked about the topmost concerns regarding an ICS cybersecurity incident, respondents predominantly mentioned the health and safety of their workers (78%) and possible damage to the quality of their products or services (77%) as significant worries should the worst happen. Experts rated the decline in consumer confidence (63%) and possible damage to equipment (52%) as substantial fears.

This research identifies the significant problem of weak authentication in IoT devices in the ICS environment. Although there are a few problems concerning ICS, this paper will specifically solve the abovementioned problem.

One of the most significant beneficiaries of ICS is mine and factory workers. For example, in a mining surrounding, sensors can relay statistics throughout the DMR Tier three community that may file if the mine is solid or dangerous chemical compounds within the air. A suitable and secure route of motion may be taken from there. In a factory where some materials need to be shaped or cut using a sharp blade, ICS can do that without human interaction, saving workers from extreme injuries.

The implications of using computerised technology to control and monitor facilities were quickly recognised by security researchers and became a concern in the mid-2000s. When dealing with the protection of digital information, put forward are usually the concerns of information confidentiality, integrity, and availability. The problem is the CIA triad of data and information security. Data protection has also become a significant compliance concern, especially in the management part of the facility. ICT networks must ensure that asset information, such as operational and financial data, is secure when using ICS. However, it can also be invaluable information for more sophisticated attacks, especially destructive attacks. Such attacks usually require a deeper understanding of how the facility`s industrial processes are coordinated. It means that we need to ensure operational reliability and security. The Aurora Generator test above shows that safety hazards can lead to destruction and directly impact human life, production, or distribution.

In this paper section, A. provides ten related works in ICS. B. system overview of ICS. C. Impact of IoT in ICS. D. significance and limitations of ICS research. E. research methodology. F. proposed a solution and in the final section the conclusion and direction for future work.

II. Literature Review/Related Work

(Asghar, Hu, and Zeadally, 2019) Investigate potential cyberattacks against ICS, point out common exposures and threats, and review unsolved security problems with present ICS cybersecurity solutions to identify problems,

technologies, and challenges. Security survey, security analysis, security monitoring, authentication, defence and countermeasures, and risk assessment were carried out. They suggest solutions to train in sets, check normal network behaviour and use that model for discovery security risk assessment. Further research is still required on IDS, Risk assessment, and metrics. In addition, the ICS security program still needs to be deployed.

(Jianxin and Dongqin, 2017) identified and analysed the threats concerning ICS. They implemented ICS security in multiple phases. They divide the process of security implementations into four stages, from low to high. They analysed industrial communication processes and SFFSM to explain it. This paper proposes a state fusion automaton model with finite states. From the perspective of analysing the characteristics of the industry, the Risks of specific target industrial control systems were also designed. More numbers of SFFSM state attributes need to be added for increased accuracy. Packet sequence efficiency and approach suggestions address risk aversion. The storage capacity in the information library should additionally be studied.

(Bhamare et al., 2020) several surveys were conducted on the safety and security of ICS, Cybersecurity risk assessment of SCDA: Cloud-based ICS systems, and [3] Mathematical tactics for dispensed filtering and management of ICS. [3] Implementation of Machine learning Algorithms, Academia. Implementation and Standardisation, Industry, and IEEE standardisation. Advanced malware control systems such as B. Zero-day attacks make it extremely tough to block and identify attacks on the ICS integrant level. [3] Hence, a brand-new scheme is needed for Intrusion detection of ICS structures throughout the procedure of Relocation of ICS from individual plans to cloud base. Developing secure cloud-based ICS Learning techniques. A hybrid dataset must be prepared; traffic dumps must be collected before and after data traffic via a firewall.

(Timpson and Moradian, 2018)**.** They suggested a methodology that balances the security and safety necessities in an ICS setting. 1. They established cognisance and framework, 2. Safety and security system planning and classification, 3. Security & safety threat assessment, 4. Evaluation and deconflict requisites, and 5. Communications and bondholder involvement. This study shows the integration and harmony of security and safety. If the requirements go beyond the coordination and separation of technical means, non-technical means should also be considered. The methodology should be demonstrated using appropriate strategies to demonstrate its feasibility in an ICS environment or an exemplary scenario for future work.

(Idrissi, Mezrioui and Belmekki, 2019). They aimed to emphasise [5] the security issues and challenges of ICS and propose the right and suitable solution. Offered an [5] overview of the architecture of the ICS and operational processes and briefly described the development of ICS. Provides analysis of potential ICS vulnerabilities and [5] suggests listing maximum associated cyber-assaults on ICS within the last ten years. Discussed difficulties and limitations in [5] IT security solutions to a secure ICS environment. Suggested guidelines and [5] a listing of the excellent Practice to enhance the safety of gadgets in ICS. Result of their research, they suggested six measures to improve ICS security. E.g., risk assessment, protect the perimeter, and Defence in-depth approach. They suggested developing a dedicated security system for future work, only for ICS.

(Tsiknas, Taketzis, Demertzis and Skianis, 2021). Their research describes attacks on industrial IoT systems and provides a complete assessment of the solutions to these attacks proposed in the latest literature. Intend to offer a more efficient and cybersecurity-focused tactic, eventually leading to a more extraordinary robust industrialised surrounding. Their study details the attacks on industrial IoT systems, considering the main characteristics and vulnerabilities of the attacks on those systems. The result of research found some countermeasures to stop cyber-attacks, e.g., URL embedding must be used to prevent phishing attacks. Future work and research suggested by Tsiknas et al. of alternative techniques of attacks or evolved strategies of combination methodology of unknown attacks such as zero-day attacks must be carried out.

Adeyanju, I. (2020) [7] Their research provides an overview of ICS threats, vulnerabilities, cyber-physical attacks, and security technologies over the past two decades from 2000 to 2019. [7] This white paper explores the latest security technologies. [7] These technologies, with careful consideration, are for ICS security researchers, asset owners, and organisations looking to develop more proactive security solutions to help combat ICS-related threat attacks and vulnerabilities. [7] The result of research for Network Configuration and communication Vulnerabilities Removable device, driver malware, authentication Bypass, Buffer overflow, Man- in -Middle attacks. Intrusion detection technology must be used to prevent his attack, and best practices to stop the attack demilitarisation and firewalls should be used. As vulnerabilities and attacks increase, more security solutions should be discovered for future work.

(Domínguez et al., 2019) [8] They endorse a method for experimentation in cybersecurity of commercial management systems, primarily based on replicating an easy commercial management system. [8] They intend to offer flexibility for an easy and stable definition of far-off or on-web web page hands-on tasks for education in ICS cybersecurity. By deploying a suitable community structure, college students can carry out tool configurations or count on extraordinary roles in the management system from automation or safety perspectives. Their findings: advantages, [8] Remote college students will have complete entry to the plans, equal to what they might have locally. The use of VMs presents flexibility when considering that faculty may want to upload lots of them as vital to define new responsibilities or refine the present ones. Furthermore, the disadvantage is that the far-off use of the device implies a cheerful lack of flexibility because all obligations regarding physical modifications, including cable reconnection or the use of the HMI panel, are manifestly unavailable. [8] Therefore, their suggestion for further research in this line must be targeted at improving efficient approaches for control and maintenance, apart from the definition of recent courses.

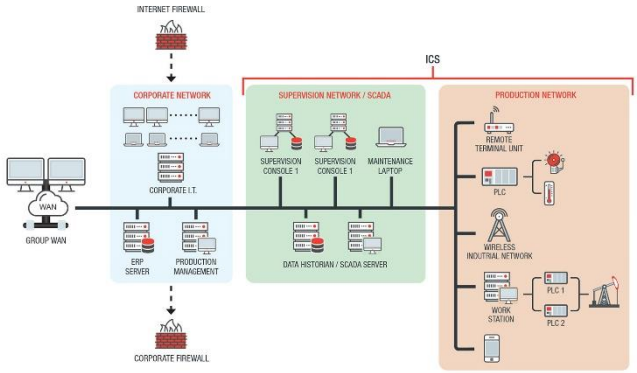
(Ferrag et al., 2017) [9] This paper presents a complete survey of authentication protocols for IoT. Specifically, greater than 40 authentication protocols evolved for or carried out within the context of the IoT are decided on and tested in detail. [9] These protocols are labelled based on the goal

environment: Internet of Vehicles, Machine to Machine Communications, Internet of Sensors, and Internet of Energy. [9] After engaging in a complete survey of authentication protocols, they found that the reliability of an authentication protocol relies upon now no longer simplest at the effectiveness of the cryptography technique used in opposition to assaults but additionally on the computation complexity and verbal exchange overhead. Future studies direction. Authentication protocols for the IoT can be progressed in phrases. [9] Capable of cowl each authentication and confidentiality and be more excellent green in terms of computation complexity and conversation overhead so long as they could cooperate with different mechanisms for detecting and warding off assaults within the IoT environment.

(M. Arafune *et al.*, 2022) [10] They inspire the distance in missing studies withinside the automation of risk searching in ICS networks. We advise an automatic extraction of risk intelligence and the technology and validation of a hypothesis. They presented an intuitive risk searching framework based on risk intelligence furnished using the ICS [10] MITRE ATT&CK framework to automate the tasks. They aim to create an automatic threat detector for the ICS environment by designing an open-source and central framework for automated threat hunting in ICS networks. The result of the proposed framework is of sizeable use for the ICS because of its novel technique for danger searching. The answer might be computerised in ICS organisations, reducing human errors, time, and usual expenses within the complex searching process. Further, the framework can offer extraordinary facts concerning the assaults primarily based on the [10] MITRE ATT&CK framework, thereby making it beneficial for ICS organisations to interpret the assaults in-depth. This kind of software is likewise not often observed within the ICS enterprise. [10] Further research suggests exploring and studying graph analysis and how it might assist the framework in improving automated threat hunting in ICS.

III. SYSTEM OVERVIEW OR ARCHITECTURE OF ICS

Today's essential industries depend on finely computerised business manipulate sectors and are operated via vital infrastructures of related and jointly based structures referred to as ICS. These are predominantly determined in industries consisting of Nuclear, Petroleum, Energy, manufacturing, automotive, chemical, food, water, electricity, pharmaceutical and mining. The period ICS contains three essential varieties of structures which consist of Distributed Control Systems, SCADA structures, at the side of the incorporation of more minor controller hardware additives consisting of the skid-established Programmable Logic Controllers (PLC). DCS is commonly determined inside a localised area, consisting of a business method plant or a factory, as a beneficial dispensed device layout predicated on supervisory and regulatory manipulation. DCS emerged as a device for controlling the structures worried past a small molecular area whilst amassing statistics in actual time on high-bandwidth/low-latency statistics networks.



2022. [image] Available at: <https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system> [Accessed 12 June 2022].

Loop control is typically extended to the top DCS controller because everything works in real-time. Such systems can be found in refineries and chemical plants, among other places. SCADA systems are designed for delivery applications that need to collect remote data over unreliable data networks. B. Those with low bandwidth / high latency connections. These systems are implemented in geographically separated locations (often scattered over thousands of square kilometres) using open-loop control with centralised data acquisition and monitoring control. Monitoring data is typically sent back to the control centre via a remote terminal unit (RTU). RTUs are typically limited to limited capacity to handle local controls when the master station is unavailable. However, as technology advances, the capabilities and performance of these RTU systems continue to improve. SCADA systems are typically used in water pipelines and the natural gas industry. PLCs are computer-based devices resulting from the technical replacement of ladder-type relay racks. These are vital components of small control system configurations and are used in almost every individual industrial process.

PLCs are typically integrated as a vital component of the DCS architecture and provide feedback or feedforward control loops that automatically maintain the desired conditions of the process around specified settings. We can set PLC settings to determine the required margins and provide the speed of self-adjustment and self-correction whenever system disruption occurs. Today, as the current ICS architecture evolves into a hybrid that integrates the capabilities of both SCADA and DCS, the boundaries between these three system definitions are blurring. The key components for working with the ICS include control loops, HMIs, and remote diagnostic and maintenance utilities. The main control components of the ICS include an intelligent electronic device (IED), a control server, MTU, RTU, SCDA server, PLC, input/output servers, and HMI.

Control networks have merged with company networks to facilitate tracking and controlling structures from the outdoor, which permits decision-makers at an agency stage to enter system data. Network topologies can range substantially from one ICS to another, with specific traits for every layer inside a managed gadget hierarchy; however, the maximum essential additives they need to consist of are: a Fieldbus community, an organised community, communications routers, a firewall, modems, and far-flung

get entry to points. Initially, ICS used specialised hardware and software programs to run proprietary management protocols, making them remoted structures with little resemblance to conventional Information Technology (IT) structures. However, IT answers are being designed into ICS to facilitate far-flung entry to skills and company connectivity. Using modern computers and community pro and low-price Internet Protocol (IP) gadgets to update proprietary answers presents new IT skills. However, it reduces the ICS isolation from the outdoor global, and for that reason growing the opportunity for cyber protection vulnerabilities and incidents. Despite providing answers to those protection problems in usual IT structures, unique issues and precomputed to be tailor-made to stabilise the ICS.

Additionally, performance and protection desires can, from time to time, war with protection withinside the layout and operation of managed structures. Because every such ICS is particular in its overall performance and reliability, everyone calls for its personal, and from time to time unconventional, running gadget and packages which is probably appeared as atypical or tough with the aid of using usual IT personnel. Implementing an ICS usually entails a few shapes of effect, which is complicated and may cross a way past the instant strategies. Some ICS traits range from conventional data processing structures because they directly affect the bodily global. These would possibly hazard human and environmental fitness and protection, in addition, to detonate monetary problems associated with manufacturing losses that may compromise proprietary data and have a terrible effect on a country's economy.

IV. Impact of Internet of Things in industrial control systems.

IoT in ICS is ending up a unique advantage for robotization organizations. Modern computerization organizations that utilise IoT arrangements can receive new advantages. The IoT assists with making innovations to improve activities, tackle issues and increment efficiency. The IoT can be made sense of as the association of incomparably recognizable electronic gadgets utilizing Internet 'information plumbing' including Internet Protocol (IP), distributed computing and web administrations. IoT Impact on ICS is exceptionally high, and it makes us utilize tablet PCs, advanced mobile phones, virtualized frameworks, distributed storage of information, etc.

Allow us to look at the effect of IoT on Industrial Control Systems:

A. Internet of Things (IoT)

IoT assumes an essential part in modern computerization as it is beginning to investigate and execute IoT ideas and innovation. IoT assists with smoothing out, breakdown, and making framework models that are viable, reasonable, and responsive. The significant point is to make frictionless interchanges and communication from assembling field input/yield including analysers, actuators, advanced mechanics and so forth to upgrade adaptability and expanded assembling. Utilizing IoT, modern robotization has utilized business advances in significant applications and these models incorporate PLCs uprooting banks of transfers.

B. Internet of Things gadgets

IoT gadgets can be utilized in different fields, and they might shift from home computerization and the usefulness of your home. Gadgets, for example, smoke alarms, indoor regulators, brilliant music frameworks, and savvy lights go under this classification. Then again, IoT gadgets are additionally present in the cooperation with the human body, where we can discuss wellness trackers, brilliant body scales or even child screens.

C. Internet of Things items

IoT is the following large innovation transformation and just web associated gadgets are proficient to assemble information. Numerous IoT items fit flawlessly into the examples of day-to-day existence by improving on routine undertakings. IoT items come in different ways, and they can be utilized in various verticals. Utilizing IoT items, business and buyer lives can be more consistent than at any time in recent memory.

D. Modern IoT Development Kits

Modern IoT Development Kits give a whole, excellent plan climate for designers and arrangement engineers to speed up the turn of events and conveyance of IoT applications radically. Utilizing these packs, any turn of events/modern climate can be immediately transformed into a creation-prepared unit. The IoT Development Kit focuses on an assortment of IoT application necessities by giving a scope of various equipment stages, crossing from exceptionally reduced low-power ARM-based plans to strong multi-centre, most recent age Intel Atom passages.

E. IoT Gateway Devices

IoT Gateway gadgets go about as a correspondence span between IoT Sensor Network and Cloud Server. IoT Gateway Devices are arising as key components in carrying cutting-edge gadgets to the Internet of Things (IoT). They help to incorporate conventions for systems administration, assist with overseeing stockpiling and edge investigation on the information, and work with information stream safely between edge gadgets and the cloud.

V. Top automation technologies in ICS

A. The Industrial Internet of Things

IIOT utilizes relevant statistics and vital obligations processed via tablets, smartphones, and different area devices. In real-time, groups can use this overall performance fact to conform and exchange their operations into a better-streamlined method externally and internally for both

lengthy-time periods and quick-term dreams. Because of this super connectivity, faster reaction instances are facilitated from all departments and allow enhanced agility for operations of all sizes. intelligent machines aren't handiest higher than people at shooting and studying records in actual time, but they may be additionally better at speaking critical records that can be used to pressure enterprise choices faster and with better precision. IIoT in manufacturing holds the impeccable ability for best control, deliver chain traceability, sustainable and green practices, and ordinary supply chain efficiency. Predictive preservation, asset tracking, progressed field carrier, greater consumer satisfaction, and facility control are the top touted blessings of IIoT.

B. The Cloud

The cloud era is new and conventional operators across industries are sceptical of its intangible nature. Because it is not maintained domestically and cannot be stored, monitored, or secured using conventional techniques, the cloud-based generation is how the businesses of the destiny will function as it allows remote workforces and in-residence to collaborate in real-time precisely in comparison with conventional records structures. One benefit of cloud technology is that the cloud technique is faster, reduces maintenance, and improves manageability. the trendy examples of innovation in industry four. Zero that has reinvigorated the producing space for organizations of each size is the Cloud ERP. The cloud ERP answers without the excessive price of on-premises answers offer appreciably advanced degrees of insight into operations by omitting the steeply-priced costs of upkeep, hardware, and safety. And with the more capital supplied by using those all-in-one solutions, the small and medium agencies are locating it less difficult to make their mark within the market, in many instances constructed particularly for her industry.

C. Robotics

The robots will command a higher presence in shaping the manufacturing enterprise as those entities turn out to be more intelligent, cost-effective, and extra efficient in their roles at the factory edge. With advances in the robotics era, those machines tackle complicated trends, including high dexterity, machine learning, memory, and the potential to collaborate more precisely. For this reason, these robots will bring in a new set of requirements that each manufacturer will want to conform to remain applicable. Robots were relied upon as a critical part of the production. Robot presence provides splendid advantages, more desirable accuracy, pace, and tireless labour, but they cannot do it all. As a result, those smaller and agiler implements in the manufacturing area are engineered to work collaboratively alongside their human counterparts and are referred to as collaborative robotics.

D. Cybersecurity

Retaining the integrity and protection of the digital structure will become a big issue as an increasing number **of** operations circulate closer to cloud-primarily based answers and depend quite adjacently on a robot workforce. Increased possibilities for threats end up more manufacturers simultaneously building and combining their systems thru the industrial net of factors. Furthermore, new technological advancements are being implemented via producers to beautify automation tactics every day. The professionals are increasingly privy to their want for heightened safety in an increasingly insecure virtual landscape, as modernization gives a couple of possibilities for boom and manner enhancement. To deal with the vulnerabilities, a better appearance is being laid at cloud-based ERP and unified systems by manufacturing and other industries. As time goes on, cloud-based ERP systems are being relied upon by way of firms of each length. Possibly, cloud-based safety is one of the fundamental subjects surrounding the efficacy of current ERP systems. It is not that security dangers don't exist inside the cloud. They're always gifts. However, besides the cost, coping with safety troubles for cloud-primarily based ERP is a complex procedure.

E. Artificial Intelligence

Artificial intelligence technology is already in our everyday lives within the shape of self-driving vehicles and business robotics. The generation in manufacturing programs becomes the new trend through which big sets of facts are analysed and predictive maintenance is passed through. Quick, to live to tell the tale, the agencies will have no preference however to "cross virtual". The AI algorithms can also be used to optimize manufacturing delivery chains, thus assisting agencies to anticipate market modifications. By seeking out patterns linking vicinity, weather patterns, customer conduct, political fame, and socioeconomic and macroeconomic elements, the AI algorithms formulate estimations of marketplace demands. The producing enterprise will have the most crucial effect of AI coupled with automation.

VI. SIGNIFICANCE AND LIMITATIONS OF THE ICS RESEARCH

A. Significance

ICS refers to the vast elegance of structures that degree, display, manipulate, and automate methods in various industries and sectors. ICS are of numerous types, PLC, SCADA, DCS, and Remote Terminal Units. They are used to display and manipulate methods in industries and sectors. Typically, those legacy structures have operator and engineering stations, essentially pc terminals. In addition, these have some cutting-edge working gadgets based on a few UNIX or Windows flavours.

When many of those structures had been designed and built, the non-public pc became a novelty, to be had best in some houses, and the net started to become famous. The control of many production corporations noticed cost in connecting those enterprises IT structures with the older legacy management structures. Likewise, it is viable that the humans at the rate of (MIS) Management Information Systems had little clue of even the life of those legacies' management structures or their vulnerabilities. Now, legacy ICS has suddenly been related to the net and thus, has become liable to cyber-attacks.

Hundreds of legacy DCS, SCADA, and PLC structures might be vulnerable to being attacked by numerous entities, such as terrorist agencies and rogue states, hacktivists, and Intruders. An assault on those structures can cripple the essential infrastructure of any organisation or country moreover motivate chaos and disruption. However, that is impossible since it will likely be an overall mission to update this vintage insecure automation structure with a new one, such as an Industrial IoT-based solution. Therefore, it has become essential to apprehend ICS security, perform a hazard evaluation of those structures, and defend them.

B. Limitations

One of the most significant limitations of this research is access to resources; some of the resources are experts in the area. It is tough to consult with an expert in ICS. Discussing the research topic with an expert would make it easy to understand the direction to do a proper study. Conducting surveys or interviewing people working or experienced in the ICS field was not possible in this research. Access to the most related and accurate literature on ICS is also limited. Most ICS-related articles do not vividly address a scientific problem and its solutions. Many research papers in ICS do not indicate the research gap.

Financial resources are also the biggest problem in this research. To do ultimate effective research, some software and hardware tools are needed to be purchased, but due to financial difficulty, alternate and least expensive ways were taken, which are not so effective in conducting the most influential research; research result is highly affected due to the above limitations. Time is also a limitation, the more time is taken to do research, the more practical information and the better result are to be found; deadlines limiting the research findings and the pressure of doing the enormous task in a small amount of time affect the outcome of the research.

VII. RESEARCH METHODS USED

This research is based on 4 phases. First, in the literature review to collect data, we assessed studies conducted by other scholars, which helped us identify what, how, and why they used specific methods for solving a problem, outcomes, and suggestions for further research. Second, in modelling, we planned to design an algorithm with logical mathematics to solve authentication problems using MATLAB. Implementation, the algorithm to be converted into suitable code to test the outcomes. Experimentation, network simulator to evaluate the performance of implemented algorithm's code versus existing algorithm.

VIII. PROPOSED SOLUTION

We have identified that the only significant problem in our research is the weak authentication of IoT devices in Industrial Control Systems. To resolve this problem, we proposed designing an enhanced authentication algorithm to increase IoT devices' security in ICS. The algorithm can decrease cyber-attacks on ICS organisations. Hence, real-life chaos can also be reduced because ICS has a massive impact on human life, like water treatment. If cyber attackers treat water inappropriately, thousands of people drinking that water may be severely harmed. Existing authentication techniques can collaborate with the proposed authentication algorithm to enhance IoT's authentication protocol in ICS. Hence, an enhanced authentication algorithm is proposed to be designed using MATLAB to strengthen the vulnerable authentication mechanisms for IoT devices in ICS. Although the has been significant research traction to improve authentication of IoT devices in ICS, there is potential for enhancement to diminish cyberattacks.

IX. CONCLUSION AND FUTUREWORK

ICS has advanced appreciably, and features are open to the Internet and handy from the outside means no air gap. However, over the years, cyber assaults on ICS structures have increased. Unsurprisingly, ICS structures are at extra risk of safety threats compromising those structures' CIA (confidentiality, integrity, and availability). Despite the latest reputation of using massive records analytics and cloud computing for ICSs, their safety remains an open issue. ICS-related industries could enjoy the cloud systems; however, loss of exemplary safety in novel multi-cloud strategies may also reason excessive expenses related to the safety breaches with the real-time enterprise systems.

In this research, we reviewed several works of literature and analysed different problems that still need to be solved in ICS. However, we only focused on one of those problems, the weak authentication of IoT devices in ICS. Therefore, we proposed a solution to design an enhanced authentication algorithm for IoT devices in ICS. For further research, the proposed authentication algorithm must be designed and implemented on the IoT devices of Industrial Control Systems.

ACKNOWLEDGEMENT

The authors thank the Tshwane University of Technology for their support. The authors declare that there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] Asghar, M., Hu, Q. and Zeadally, S., 2019. Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165, p.106946.

[2] Xu, J. and Feng, D., 2017. Identification of ICS Security Risks toward the Analysis of Packet Interaction Characteristics Using State Sequence Matching Based on SF-FSM. Security and Communication Networks, 2017, pp.1-17.

[3] Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K. and Meskin, N., 2020. Cybersecurity for industrial control systems: A survey. *Computers & Security*, [online] 89, p.101677. Available at: <https://www.researchgate.net/publication/339199590_Cybersecurity_for_Industrial_Control_Systems_A_Survey?enrichId=rgreq-6dbb79aef51f1a08568e89fdc7fa006f-XXX&enrichSource=Y292ZXJQYWdlOzMzOTE5OTU5MDtBUzo4NzIyMjg1Njg3MDcwNzRAMTU4NDk2NjkwNDc3MA%3D%3D&el=1_x_2&_esc=publicationCoverPdf>.

[4] Timpson, D. and Moradian, E., 2018. A Methodology to Enhance Industrial Control System Security. Procedia Computer Science, 126, pp.2117-2126.

[5] Idrissi, O., Mezrioui, A. and Belmekki, A., 2019. *Cyber Security Challenges and Issues of Industrial Control Systems–Some Security Recommendations*. [online] Ieeexplore.ieee.org. Available at: <https://ieeexplore.ieee.org/document/9071701/>.

[6] Tsiknas, K., Taketzis, D., Demertzis, K. and Skianis, C., 2021. Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *IoT*, 2(1), pp.163-186.

[7] Abeyanju, I., et al. 2020. [online] Available at: <https://www.researchgate.net/publication/344107065_Digital_Industrial_Control_Systems_Vulnerabilities_and_Security_Technologies> [Accessed 24 May 2022].

[8] Domínguez, M., Morán, A., Alonso, S., Prada, M., Pérez, D. and Fuertes, J., 2019. Experimentation environment for industrial control systems cybersecurity: On-site and remote training. *IFAC-PapersOnLine*, [online] 52(9), pp.248-253. Available at: <https://www.sciencedirect.com/science/article/pii/S2405896319305464>.

[9] Ferrag, M., Maglaras, L., Janicke, H., Jiang, J. and Shu, L., 2017. Authentication Protocols for Internet of Things: A Comprehensive Survey. *Security and Communication Networks*, [online] 2017, pp.1-41. Available at: <https://doi.org/10.1155/2017/6562953>.

[10] M. Arafune *et al*., "Design and Development of Automated Threat Hunting in Industrial Control Systems," *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, 2022, pp. 618-623, doi: 10.1109/PerComWorkshops53856.2022.9767375.

[11] Jablonski, D., 2021. The Top 3 Cybersecurity Issues for Industrial Control Systems in 2021. [online] Gca.isa.org. Available at: <https://gca.isa.org/blog/the-top-3-cybersecurity-issues-for-industrial-control-systems-in-2021> [Accessed 2 March 2022].

[12] Hossain, N., Das, T., Islam, T. and Alam Hossain, M., 2021. Cyber security risk assessment method for the SCADA system. Information Security Journal: A Global Perspective, pp.1-12.

[13] Arockiam, L & Joshitta, R. Shantha. (2016). Authentication in IoT Environment: A Survey. international Journal of Advanced Research in Computer Science and Software Engineering. 6. 140-145.

[14] Diaz, T., 2022. [online] Study.com. Available at: <https://study.com/learn/lesson/industrial-control-systems-ics-concept-examples.html#:~:text=Industrial%20Control%20Systems%20(ICSs)%20refer,processes%20in%20the%20production%20chain.> [Accessed 31 May 2022].

[15] Alizai, Z., Tareen, N. and Zadoon, I., 2018. *Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures*. Islamabad.

[16] Plantautomation-technology.com. 2022. *Impact of Internet of Things (IoT) on Industrial Automation*. [online] Available at: <https://www.plantautomation-technology.com/articles/impact-of-internet-of-things-on-industrial-automation> [Accessed 6 July 2022].