IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

SCADA Systems: Vulnerabilities and Blockchain Technology

Gandharv Kumar, Jatin Chawla,Vimmi Malhotra
Dronacharya College of Engineering, Gurgaon, Haryana, India

Abstract: *One of the most crucial components of industrial operations is SCADA systems.Prior to SCADA, industrial process monitoring and control had to be done by plant staff using selection switches, pushbuttons, and knobs for analog signals. Relays and timers were utilized to help with supervision as production increased and sites spread farther apart. With the development of technology and the introduction of network-based protocols, these systems got more dependable, quick, and troubleshooting became simpler. Indeed, vulnerabilities accompany growth, which was nothing new for SCADA. The security of these systems was put at risk by the IP protocols. The attack by the Stuxnet virus may serve as an example of the destruction that SCADA might suffer at the hands of cyber predators. This essay examines SCADA systems' definition, applications, and protocol usage.*

Keywords: SCADA systems, Vulnerabilities, blockchain technology, decentralization

I. INTRODUCTION

SCADA stands for Supervisory Control and Data Acquisition. It is a collection of both software and hardware components that allow supervision and control of production plants, both locally and remotely and is used to gather real time data. It consists of HMIs (Human Machine interaction) which facilitates interaction with field devices such as pumps, valves, motors, sensors etc. SCADA software usually links the databases and HMIs. The structural design of a standard SCADA system starts with RTUs (Remote terminal Units) or PLCs (Programmable Logic Controllers). RTUs and PLCs are microprocessors that communicate with field devices and HMIs. The data from RTUs and PLCs is then routed to SCADA computers where software interprets and displays the data to operators for analyzing and reacting to system events.

Before SCADA, monitoring and control was the task of plant personnel. In the 1960s, with the growth of manufacturing, telemetry came on the scene to offer automated communication. In the 1970s, the term SCADA was coined for standalone units with PLCs and microprocessors without networking. Later in 1990s and 2000's SCADA system started to implement open system architectures with communication protocols allowing real time plant information to be accessed anywhere around the world. With SQL, data history can be logged and used in trending applications and record keeping. On HMI and end user computer, graphical representation of operations exist for operator interactions. Data may be analysed and used to enhance plant production and troubleshoot problems.

II. USES OF SCADA SYSTEMS

The usage of these systems in industrial organisations including telephony, oil and gas refinery, and transportation

Water and waste management, for example, since they support efficiency maintenance and data processing for wiser action. Electric power generation, distribution, and transmission all use SCADA systems to detect current flow and line voltage. Manufacturing facilities successfully employ these systems to regulate industrial automation, monitor the workflow, and maintain process quality.

Additionally, all operations relating to railroad trains and trolleybuses are automated, monitored, and controlled via SCADA. These systems are used by waste water and sewage utilities, power plants, and businesses like the forestry, pulp, and paper sectors to monitor and manage the water pump station.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

III. PROTOCOLS USED IN SCADA SYSTEMS

The usage of these systems in industrial organizations including telephony, oil and gas refinery, and transportation Water and waste management, for example, since they support efficient maintenance and data processing for wiser action. Electric power generation, distribution, and transmission all use SCADA systems to detect current flow and line voltage. Manufacturing facilities successfully employ these systems to regulate industrial automation, monitor workflow, and maintain process quality.

Additionally, all operations relating to railroad trains and trolleybuses are automated, monitored, and controlled via SCADA. These systems are used by wastewater and sewage utilities, power plants, and businesses like the forestry, pulp, and paper sectors to monitor and manage the water pump station.

No matter what protocols are used for the incoming data, the packets are created. TCP/IP networks share Ethernet and frame relay networks' packet characteristics. As it is connection orientated, it needs to establish the connection before transferring data. The server replies to the client's inquiries once the connection is made and continues to do so until the client cuts the connection.

IV. VULNERABILITIES OF A SCADA SYSTEM

Many Vulnerabilities, including hackers, personnel who aren't security-conscious, malware, and a lack of software and hardware maintenance, can be a hazard to such systems. Threats to critical infrastructure include theft, terrorism, accidents, crimes, and natural disasters. These might be the causes of such systems failing. As a result, these systems must be made reliable and should be regularly maintained. The software is more vulnerable than hardware losses and attacks since hackers and other cyber predators are one step ahead of them. A danger analysis states that 60% of these sites don't use anti-virus protection, which increases the possibility of automatic signature updates. Around 70% of websites employ passwords that are simple to crack, which puts users at risk for manipulation, denial of service, and data interception.

There may be hackers who gain access to the SCADA network may make some unauthorized changes to instructions and commands by compromising the servers. This could be an act of outsider or insider where different information to operators and control systems could be presented. Majority of SCADA network have Master Stations which can control the systems and if these stations are not protected by firewalls, antivirus or other methods can lead to undesirable conditions. Equipment protection systems could be messed up and can lead to destruction in costly and irreplaceable equipment. Interference in safety system canal so endanger human life.

V. COMBATING SCADA VULNERABILITIES

With the usage of client–server based protocols, the problem of security of the network is encountered. The prominent challenge is to restrict the unauthorized access. Then comes the question of enhancing security inside the SCADA network and to develop security monitoring tools. Focus should also be diverted to cryptography and key management along with the device and operating system security management. There is very little emphasis on standard security methods like encryption and authentication. A robust protection strategy is the need ofthe hour for such systems. It is high time to realize the importance of implementing security programs. Some strategic steps may include removing of unnecessary functionalities and mapping of current systems and knowing all points of entry and exit which pose as threats are much easier to monitor. Secondly, early detection of potential attacks can limit the amount of damage done. Constant security checks and risk assessments should be conducted timely. Many techniques like encryption and firewalls can protect such systems. Clever techniques like “honey pots” can deal in some manner to counteract unauthorized access attempts. As many SCADA Systems use master control systems which become an easy prey for the cyber predator to attack. These systems can also be decentralized and made more reliable and safe.

VI. BLOCKCHAIN: A SOLUTION FOR CYBER THREATS

One way to make SCADA secure is by making the system decentralised because decentralisation will reduce dependence on a particular master station for controlling and monitoring operations. Blockchain is a distributed database which maintains records of all device transactions data on a SCADA blockchain network. Basically, blockchain comprises of two words where block means digital information and chain means storage in public database.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

The blocks have three main parts of information that is information about transaction for example duration and amount of purchase from any e-commerce site. Secondly, it contains information about end user who is participating in transaction and also the information to differentiate it from other blocks. The data is stored in blocks forming a linear sequence where each block references the hash of the previous block. A hash is a unique ID of a block. Anybody who tries to temper with the hash needs to change all the hashes of successive blocks which makes it a tedious task and therefore the data becomes temper proof. The working of this technology combines three leading technologies that are cryptographic keys which could be private as well as public, a peer-to-peer network containing a shared ledger and a machine which is used to store transaction and records of the network. The cryptographic keys produce a secure digital reference and play an important role in successful transaction between two parties removing the need for third party. This secure identity is called digital signature in case of crypto currency. The digital signature is combined with peer-to-peer network where large amount of individuals act as authors and transactions are carried out efficiently. Advantage of the Blockchain is the greater throughput of the database technology, faster data Communication technology, efficient consensus mechanism to make sure the security of SCADA. These transactions data are time stamped and can be checked whether the sender's data and the receiver's is validated. Also blockchain use efficient consensus mechanisms and algorithms which ensures that legitimate transactions are added and synchronizes and audits them. These consensus protocols are necessary for correct functioning of blockchains. Some of these mechanisms are Proof of Work (POW), Proof of stake (POS), Proof of capacity (POC) and Proof of Elapsed Time (POET) etc. POW is also known as mining and requires solving of complex and asymmetric mathematical puzzles. These puzzles are solved on a hit and trial basis and depends upon good computational power. The difficulty of the puzzles depends upon how fast the blocks are mined. POS is a randomized process in which producer of next block is determined. This method is energy efficient and validators actually maintain the network as they hold the coins of blockchain they are validating on. In a delegated proof of stake method users can vote for a particular delegate. A person or organisation that wishes to add blocks to a network refers to a delegate. This method is also called digital democracy. POC is another method which uses plotting whoever having the fastest solution of puzzle creates a new block. POET is a protocol inwhich assignment of random wait time to each node is done. Hence blockchain has very crucial features like transparency, encryption and accountability. This means that no single node or group of nodes can take up majority of the set andno one can change entire SCADA network software system without the majority of the entire network of users accepting the change, thus ensuring no harm to the system.

VII. CONCLUSION

Use of network protocols in SCADA systems make them vulnerable to cyber attacks. Hence a robust protection strategy is the need of the hour. Blockchain technology being a distributed, encrypted and secure mechanism can be used to ensure security of the system. As blockchain use consensus mechanism to add new transactions, it would not be easy for attackers to change data and present wrong logs thus reducing risks of scada systems.

REFERENCES

[1]. Stephen Kaisler, Frank Armour, J. Alberto Espinosa,William Money, "Big Data: Issues and Challenges MovingForward",IEEE,46thHawaiiInternationalConferenceonSystemSciences,2013.
[2]. Sam Madden, "From Databases to Big Data", IEEE,Internet Computing, May-June2012.
[3]. KapilBakshi,"ConsiderationsforBigData:ArchitectureandApproach",IEEE,AerospaceConference,2012.
[4]. SachchidanandSingh,NirmalaSingh,"BigDataAnalytics",IEEE,InternationalConferenceonCommunication,Information&ComputingTechnology(ICCICT), Oct. 19-20, 2012.
[5]. F.N. Afrati and J.D. Ullman. Optimizing joins in a map-reduce environment. In Proceedings of the 13th EDBT, pages99–110,2010.
[6]. S.Babu.TowardsautomaticoptimizationofMapReduceprograms.InProceedingsofthe1stACMsymposiumonCloudcomputing,pages137–142, 2010
[7]. A.Floratou et al . Column-Oriented Storage TechniquesforMapReduce.Proceedings oftheVLDB,4(7),2011.
[8]. C.T.Chu,S.K.Kim,Y.A.Lin,Y.Yu,G.R.Bradski, A.Y. Ng, and K. Olukotun. Map-reduce for machine learningonmulticore. pages 281–288. MITPress,2006.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

[9]. J. Dean and S. Ghemawat. Mapreduce: simplified data processing on large clusters.

[10]. R.GrossmanandY.Gu.Dataminingusinghigh-performancedata clouds:experimentalstudiesusingsector and sphere. In KDD '08: Proceeding of the 14th ACM SIGKDDinternationalconferenceonKnowledge discovery anddatamining,pages920– 927,NewYork, NY, USA, 2008. ACM.