**Cyber Threats in Mining Industry**

**Contents**

Introduction 3

WHAT MAKES Mining Industries prone to Cyber attacks ? 5

Who all are Interested in the Mining Industry data? 6

Few threats that can be observed in the mining industry 8

if security against cyber security is not taken care of? 10

the ways in which Industries can be protected from Cyber Attacks? 12

Conclusion 14

**References**

**Acknowledgment**

I would like to express my very great appreciation to Vivek Sir from the Microsoft Cybersecurity Engage team for his valuable and constructive suggestions during the planning and development of this research work. His willingness to give his time so generously has been very much appreciated.

I would also like to thank the following organizations for encouraging me to do research in such a fascinating and innovative area :

* Microsoft Team
* Cummins Teachers

# **Introduction**

Mining is the extraction of minerals or other geological materials from the earth. The process often involves mining of ores and metals, but it also includes the extraction of coal, lignite, oil shale, gemstones, sand, gravel, rock salt and construction aggregates. Mining has been around for thousands of years. From ancient times to modern day technologies have been applied to mining to increase efficiency and production levels.

This industry is a significant contributor in the global economy and has increased significantly over the past few decades.

The mining industry in India is a huge market with a lot of potential. The government is also planning to make the sector more attractive by reducing taxes and making it easier for investors to set up mines in the country.

The software technology used in this sector includes exploration software, design software, modelling software, simulation software, engineering software and optimization software among others. Cybersecurity is a major concern for the mining industry. With cyberattacks, companies can lose their intellectual property, sensitive data, and even their entire database system. Mining is one industry that has fully embraced automation due to its high production requirements which allows companies to get more value out of their efforts.

Automation in mining is the use of computers, robots, and other such devices to perform activities that were previously done by humans. Automation in mining is a new trend that has been on the rise for a while now. With the advent of AI and robotics, automation in mining can be achieved more efficiently and with less risk than before. The automation in mining has led to higher productivity and lower costs. The introduction of AI technology has made it even more efficient by automating tedious tasks such as drilling, loading, and hauling ore from different mines to a central place for processing.

However, there are some drawbacks to automation as well - it is not always reliable and can lead to increased safety risks.

# 

# **The loop-holes in Mining Industries, making them prone to Cyber attacks ?**

It is a key industry that ensures food and water security, economic stability, and social progress. Cyber attacks are on the rise against this industry. This is because mining companies generate a lot of money. They also have a lot of data about their operations which can be used to make more profit by stealing information from these companies. This rise in cyber-attacks is due to increased competition, increased demand for minerals and metals, as well as improvements in technology which makes it easier for hackers to access systems with higher computing power. There are many reasons why cyber attacks targeting mining industry has become so popular - it is an easy target, they have a lot of data that can be stolen, they have less security measures than other industries. Cyber attacks against the mining industry have been on the rise since 2013. In that year, hackers stole a wallet with 50 bitcoins from a company named the Double Trouble Casino. This was one of many cases involving this specific company and their downfall due to cyber attacks. Since then, there have been many more cases of cyber attacks on the mining industry.

# 

# **Who all are Interested in the Mining Industry data?**

* **Nation States**

As perpetrators of cyber-attacks or cyber-based interference, nation states may wish to gather intelligence, and cyber assets are increasingly being used as the primary means of doing so. Governments in developed countries have developed sophisticated and stealthy cyber assets that can collect and transmit data for years without being detected inside organizations. Cyber spying is being used by developing countries as a quick and cost-effective way to improve their intelligence-gathering capabilities.

* **Organized Cybercriminal Syndicates**

Criminal gangs can be divided into two categories when it comes to intrusions. Criminal gangs in the first category steal and sell sensitive information, encrypt sensitive documents and demand a ransom, compromise computers and turn them into botnets, and so on. Criminal gangs, who have been hired by national governments to conduct cyber espionage campaigns or carry out politically motivated disruptive or destructive cyber-attacks, fall into the second category. National governments maintain plausible deniability in the event of discovery by enlisting the help of criminal gangs. There may be a point where these two categories intersect and easy profit can be made.

* **Competitors**

Competitors spying on one another can be traced all the way back to the dawn of commerce. Intellectual property, production methods, true production capacity, pricing information, and customer information are just a few of the topics that competitors are interested in. In extreme cases, competitors may launch disruptive or destructive cyber-attacks against one another in order to gain a competitive advantage or overcome a disadvantage.

* **Hacktivists**

Hacktivists are online activists who use the internet to make a difference. They target cyber assets to bring attention to their political causes, and they frequently target high-profile or high-visibility targets. Frequently, their stated causes do not correspond to their stated goals. Hacktivists frequently target mining and oil and gas companies, protesting their impact on the environment, wildlife habitat, corporate greed, and other issues.

# **Few threats that can be observed in the mining industry:**

* **Cyber Espionage**

According to a recent cyber security report, most mines are targeted for intelligence gathering. In fact, 96 percent of attackers had this motivation.

For good reason, nation-state-sponsored hackers and corporate interest groups regard mining companies as data treasure troves. Details on the location and value of natural deposits can be found in geological exploration research. Pricing information and details on proprietary extraction and processing technology can be found in corporate strategy documents.

In M&A negotiations, insight into business strategies and mine value could be used to lower the acquisition target's price or outbid a competitor. Intellectual property (IP) and trade secrets can be used to cut R&D costs and gain a long-term competitive advantage.

* **Phishing Attacks**

In the mining industry, phishing campaigns have become more common, with malware disguised as a link or attachment in an email. They are intended to deceive a user into disclosing confidential or personal information, which can then be used fraudulently.

Senior executives, operations supervisors, control system supervisors, instrumentation technologists, and equipment diagnostic leads are among the groups or individuals increasingly targeted by phishing campaigns.

Phishing attacks have already proven to be devastating in the mining industry. The theft of over 14 gigabytes of corporate data occurred in April 2016 during an attack on Goldcorp, a Canadian mining company. Furthermore, an email phishing attack on a German steel mill in 2014 caused "massive damage" to the plant's production systems.

* **Third-party Access**

Third-party vendors are frequently used by mining operations to provide support services such as equipment assembly and maintenance. Suppliers, on the other hand, may not adhere to the standard cyber security practises required to safeguard an interconnected network.

If a vendor connects a malware-infected USB drive or laptop to the network, for example, malicious software can cross the IT/OT divide and compromise a mining company's OT system. Vendors may also expose systems by allowing users to log in with weak credentials on maintenance and other software programmes.

Third-party vendors can be the source of either intentional or unintentional cyber threats. Vendor access to internal systems, on the other hand, puts production, equipment, and corporate data at risk if not properly managed and audited. Hackers could easily infiltrate the ICS environment if one weak point in the network is combined with access by multiple vendors.

# **What can happen if security against cyber security is not taken care of in Mining Industries ?**

Let's say your IT network was hacked via phishing, and the hackers were able to gain administrative access to your OT (operational technology) system and ICS equipment. They'll have full control over your mine's monitoring systems, ventilation units, on-site pipeline or gas monitors, and automated equipment.

So, it's clear that a cyber breach, whether intentional or unintentional, has serious consequences for a mining company. It has the potential to cause mine system failure and, as a result, jeopardise worker and community safety.

When a mining company has few or no cyber security protocols in place, criminals can easily gain access to its data through phishing and social engineering. This frequently results in the theft of confidential information or the inability to access operation software, resulting in the shutting down of operations and the loss of revenue.

Customers begin to doubt a company's capabilities after it has suffered a data breach. This is one of the first signs of a company's demise. Some companies are able to recover from data breach scandals after years, but others are not so fortunate.

Customer loyalty is harmed, and sales suffer as a result. Customers generate revenue, and when your data and system are hacked, held for ransom, or stolen, it degrades customer service and has a negative environmental impact, resulting in customer loss.

Lack of cyber-Security can lead to Shutdowns in Infrastructure. For example, due to a lack of authentication, a hacker found your credentials for sale on the dark web and was able to hijack into the mine's system using your admin access, taking full control of our tailing and ventilation units, monitoring and automated systems, putting people and the environment at risk.

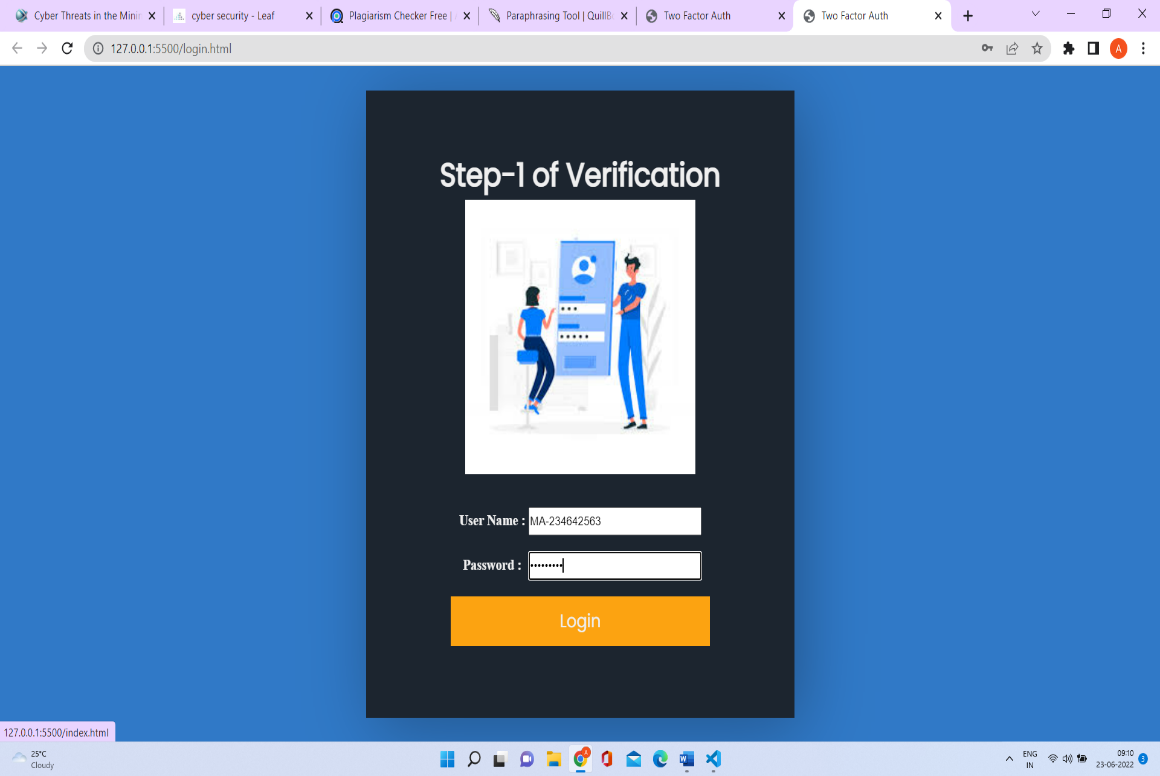
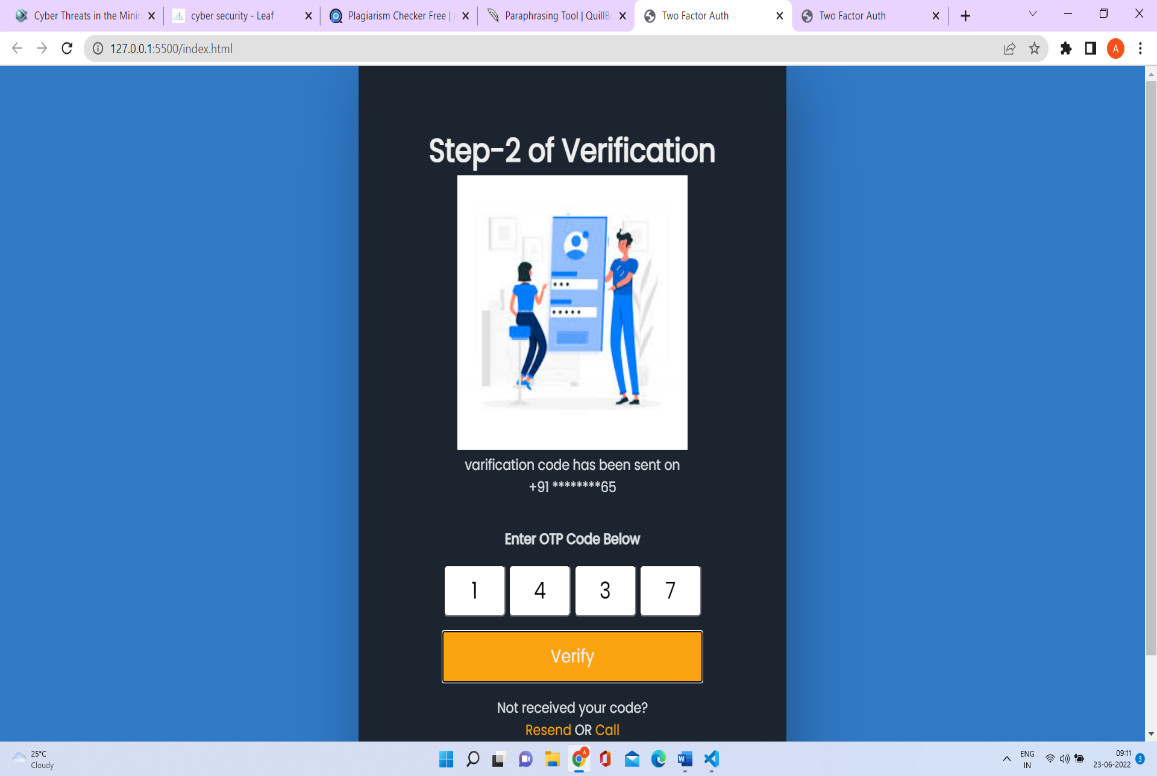
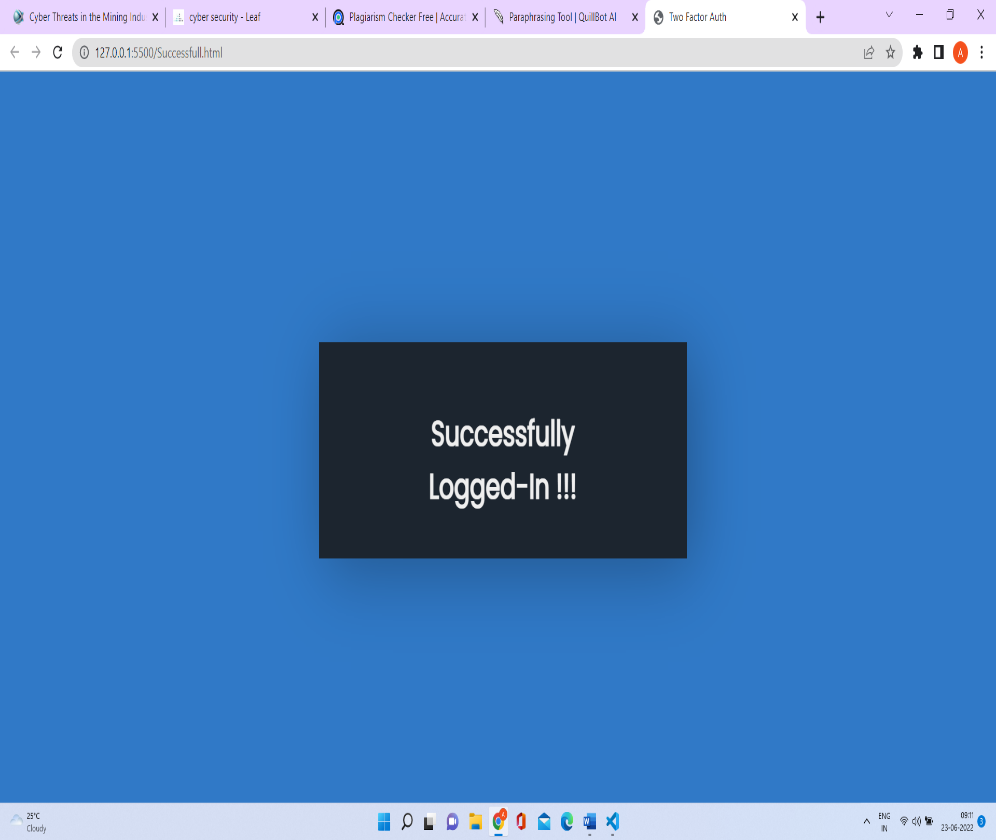
A data breach can completely disrupt the production process if proper mining IT protocols are not in place, forcing executives to shut down mining operations until the breach is mitigated. In the worst-case scenario, a hacker with complete remote access to your PLCs (programmable logic controllers), OT, and ICS equipment can completely disrupt your operations without you even realising it until it's too late.

# **What are the ways in which Mining Industries can be protected from Cyber Attacks ?**

* Two-Step Authentication

Two-Step authentication is an additional layer of protection that calls for more than one authentication mechanism to be used during a log-in. Because of this, even if someone knows your password, they cannot access your account or device.

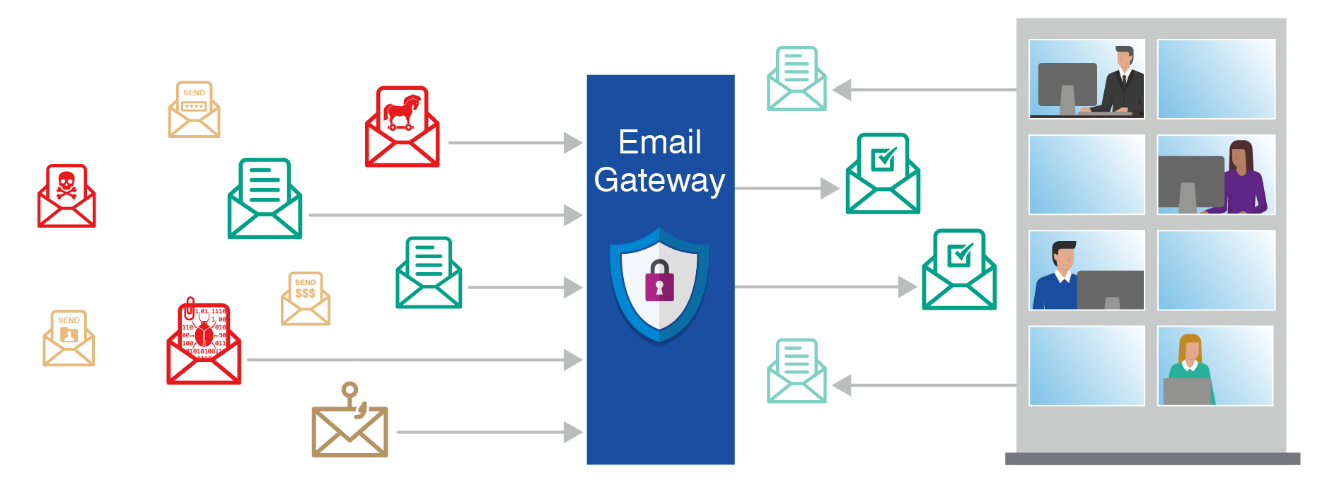
I have coded an interface for the same, whose code’s link has been shared.



* Secure the email

Implementing a secure email gateway is among the first best practises that businesses should adopt. All incoming and outgoing email is scanned and processed by an email gateway, which also ensures that threats are not permitted. Standard security methods, such as preventing known harmful file attachments, are no longer effective due to assaults becoming more complex. Deploying a secure email gateway that employs a multi-layered strategy is a superior choice.

A more secure way is to automatically and by default do email encryption.



Source: https://www.proofpoint.com/sites/default/files/email\_security\_best\_practice.png

* Apply web gateway

By enforcing organisational security guidelines and instantly filtering dangerous internet traffic, a secure web gateway provides defence against threats to online security. A secure online gateway should have URL filtering, application controls for web applications, and the ability to identify and block dangerous code, at the very least.

# **Conclusion**

The mining industry in India is a huge market with a lot of potential. The software technology used in this sector includes exploration software, design software, modelling software, simulation software, engineering software and optimization software among others. Cybersecurity is a major concern for the mining industry. The automation in mining has led to higher productivity and lower costs. Governments in developed countries have developed sophisticated and stealthy cyber assets that can collect and transmit data for years without being detected inside organizations. Cyber spying is being used by developing countries as a quick and cost-effective way to improve their intelligence-gathering capabilities. Criminal gangs steal and sell sensitive information, encrypt sensitive documents and demand a ransom.

Competitors spy on one another. They target cyber assets to bring attention to their political causes, and they frequently target high-profile or high-visibility targets. For good reason, nation-state-sponsored hackers and corporate interest groups regard mining companies as data treasure troves. Details on the location and value of natural deposits can be found in geological exploration research. In the mining industry, phishing campaigns have become more common, with malware disguised as a link or attachment in an email. They are intended to deceive a user into disclosing confidential or personal information, which can then be used fraudulently. Phishing attacks have already proven to be devastating in the mining industry. A cyber breach, whether intentional or unintentional, has serious consequences for a mining company. It has the potential to cause mine system failure and, as a result, jeopardise worker and community safety. When a mining company has few or no cyber security protocols in place, criminals can easily gain access to its data through phishing and social engineering. This frequently results in the theft of confidential information or the inability to access operation software, resulting in the shutting down of operations and the loss of revenue. Customers begin to doubt a company's capabilities after it has suffered a data breach. This is one of the first signs of a company's demise. Customers generate revenue, and when your data and system are hacked, held for ransom, or stolen, it degrades customer service and has a negative environmental impact, resulting in customer loss. Lack of cyber-Security can lead to Shutdowns in Infrastructure. A data breach can completely disrupt the production process if proper mining IT protocols are not in place, forcing executives to shut down mining operations until the breach is mitigated. Two-Step authentication, enforcing organisational security guidelines, secure web gateway provides defence against threats to the cyber safety of mining industry.

# **References**

<https://www.forbes.com/sites/forbesbusinesscouncil/2021/04/16/cybersecurity-and-nation-state-threats-what-businesses-need-to-know/?sh=551fccce7c21>

<https://www.hq.nasa.gov/iwgsdi/Mining_Industry.html>

<https://www.mckinsey.com/industries/metals-and-mining/our-insights/behind-the-mining-productivity-upswing-technology-enabled-transformation>

<https://www.mining-technology.com/analysis/featureten-technologies-with-the-power-to-transform-mining-4211240/>

<https://www.mining-technology.com/analysis/cybersecurity-in-mining/>

<https://www.mining.com/as-cyber-threats-rise-how-vulnerable-are-mining-companies/>

<https://gmggroup.org/groups/cybersecurity-working-group/>

<https://www.forcepoint.com/cyber-edu/secure-web-gateway-swg>

<https://leaf-it.com/it-services/cyber-security/>

<https://www.xybersolutions.com.au/blog/cyber-threats/>

<https://www.global.weir/newsroom/news-articles/q3-trading-update-and-cybersecurity-incident/>

<https://www.sciencedirect.com/science/article/abs/pii/S0020025520302280>

# Cybersecurity: What Everyone Needs to Know - By Peter W. Singer, Allan Friedman

# Data Mining Methodology in Support of a Systematic Review of Human Aspects of Cybersecurity - [Brendan M. Duffy](https://link.springer.com/chapter/10.1007/978-3-030-49907-5_17#auth-Brendan_M_-Duffy), [Vincent G. Duffy](https://link.springer.com/chapter/10.1007/978-3-030-49907-5_17#auth-Vincent_G_-Duffy)