

# **ANALYZING THE DIGITAL CERTIFICATES OF DOMAIN NAMES USING OSINT TOOLS**

**BY**

**SOMKENE RICHARD**

**3rd NOVEMBER, 2024**

## **EXECUTIVE SUMMARY**

The digital certificates of the domains [www.cyberagent.co.jp](http://www.cyberagent.co.jp), [www.thespargroup.com](http://www.thespargroup.com), and [www.tesla.com](http://www.tesla.com) were analyzed using OSINT tools including Virustotal, whoer.net and Abuseipdb, to verify the identity and authentication of these domains. The certificates were issued by reputable Certificate Authorities and showed valid expiration dates, with secure encryption standards in place. Alongside the certificates, the IP addresses of these domains were also examined, all of which corresponded, confirming the authentication of each domain. Additionally, the hosting providers and geolocation data aligned with the domains' verified identities, adding an extra layer of trustworthiness. In conclusion, the results suggest that these domains are secure and safe to interact with.

## **INTRODUCTION**

Digital certificates, also known as SSL/TLS certificates, are electronic files that verify a website's identity and enable secure, encrypted connections between the site and its users. These certificates are issued by trusted third-party organizations called Certificate Authorities after confirming the website owner's identity.

Analyzing digital certificates is a proactive measure against cyberattacks, such as certificate spoofing, certificate authority compromise and others. This digital certificate analysis also helps identify vulnerabilities, like expired certificates.

## **TOOLS**

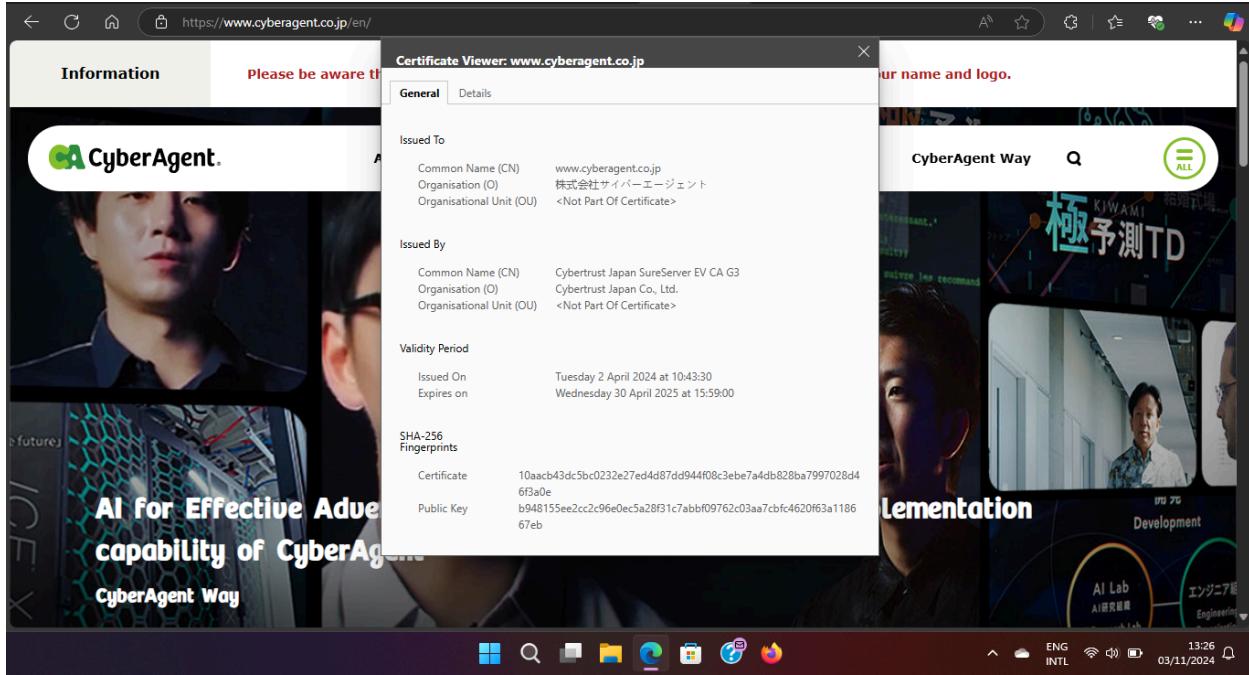
Virustotal

whoer.net

Abuseipdb

## ANALYSIS

### A. cyberagent.co.jp



An Overview of the certificate viewer, showing important details of the website

First Submission: 2014-08-27 00:51:13 UTC  
Last Submission: 2024-06-11 01:57:11 UTC  
Last Analysis: 2024-06-11 01:57:11 UTC

HTTP Response

Final URL: https://www.cyberagent.co.jp/

Serving IP Address: 163.44.161.169

Status Code: 200

Body Length: 140.00 KB

Body SHA-256: c8bd7281fe58783ab8a9cd8850d6fc7f7e724ad72f948d5d15a4e3542a990ad9

Headers

X-XSS-Protection	1; mode=block
x-rcms-cache-expire	2024-06-11 11:16:42
Strict-Transport-Security	max-age=7776000

The url was scanned on virustotal.com to reveal its IP address (163.44.161.169)

No security vendor flagged this IP address as malicious

Community Score: 0 / 94

163.44.161.169 (163.44.160.0/19)  
AS 7506 (GMO Internet, Inc)

JP Last Analysis Date: 23 days ago

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic Properties

Network	163.44.160.0/19
Autonomous System Number	7506
Autonomous System Label	GMO Internet, Inc
Regional Internet Registry	APNIC
Country	JP
Continent	AS

The IP was further scanned for more details of the domain

The screenshot shows a web browser window with multiple tabs open. The active tab displays the details of the last HTTPS certificate for the IP address 163.44.161.169. The certificate information includes:

- JARM Fingerprint:** 29d29d20d29d21c42d42d00042d58c7162162b6a603d3d90a2b76865b53
- Last HTTPS Certificate:**
- Data:**
  - Version: V3
  - Serial Number: 237a911f6ccb216102bb1dfdfdebfb8b41e3a1de4
  - Thumbprint: bd15628306faf2483bc95261ebcccd355a52e2087
- Signature Algorithm:** Issuer: C=JP, O=Cybertrust Japan Co., Ltd., CN=Cybertrust Japan SureServer EV CA G3
- Validity:**
  - Not Before: 2024-04-02 09:43:30
  - Not After: 2025-04-30 14:59:00
- Subject:** 1.3.6.1.4.1.311.68.2.1.3=JP, 2.5.4.5=0110-01-034156, 2.5.4.15=Private Organization, C=JP, ST=Tokyo, L=Shibuya-ku, O=株式会社サイバーエージェント, CN=www.cyberagent.co.jp
- Subject Public Key Info:**
  - Public Key Algorithm: RSA
  - Public-Key: (2048 bit)
  - Modulus:  
c8:80:a5:dc:c0:f4:f5:ce:d5:7e:46:b8:85:37:38:  
ed:d8:a6:88:00:da:dd:a5:c4:90:f6:e5:29:f8:13:  
36:46:8e:84:21:fc:d6:c4:57:77:af:7c:94:f5:42:  
49:3e:f2:05:78:5a:34:e5:8c:3d:55:bf:07:64:09:

The scanned IP address shows the same certificate details as seen on the certificate viewer

The screenshot shows the Whoer.net website interface. The main content area displays the following information for the IP address 163.44.161.169:

IP address: 163.44.161.169	
Location:	Japan (JP), N/A
Region:	N/A
City:	N/A
ZIP:	N/A
Hostname:	v163-44-161-169.b00c.g.tyo1.static.cnode.ioN/A
IP range:	163.44.160.0 - 163.44.191.255
ISP:	GMO Internet
Organization:	GMO Internet
Blacklist:	Yes ()
TOR:	No
Zone:	Asia/Tokyo
Local:	Mon Nov 4 2024 00:30:33 GMT+0900 (JST)

Further scanning on Whoer check for more verification and authenticity including its geolocation (Tokyo, Japan)

The screenshot shows a web browser window with multiple tabs open at the top, including "GBPC", "Cyber", "somk", "Alpha", "cyber", "Cyber", "Home", "J.P.M", "Virus", "Whois", and "163.44.161.169". The main content area is titled "AbuseIPDB » 163.44.161.169". A search bar at the top has the IP address "102.91.4.11" entered and a "CHECK" button. Below the search bar, a message says "163.44.161.169 was not found in our database". A table provides details about the IP address:

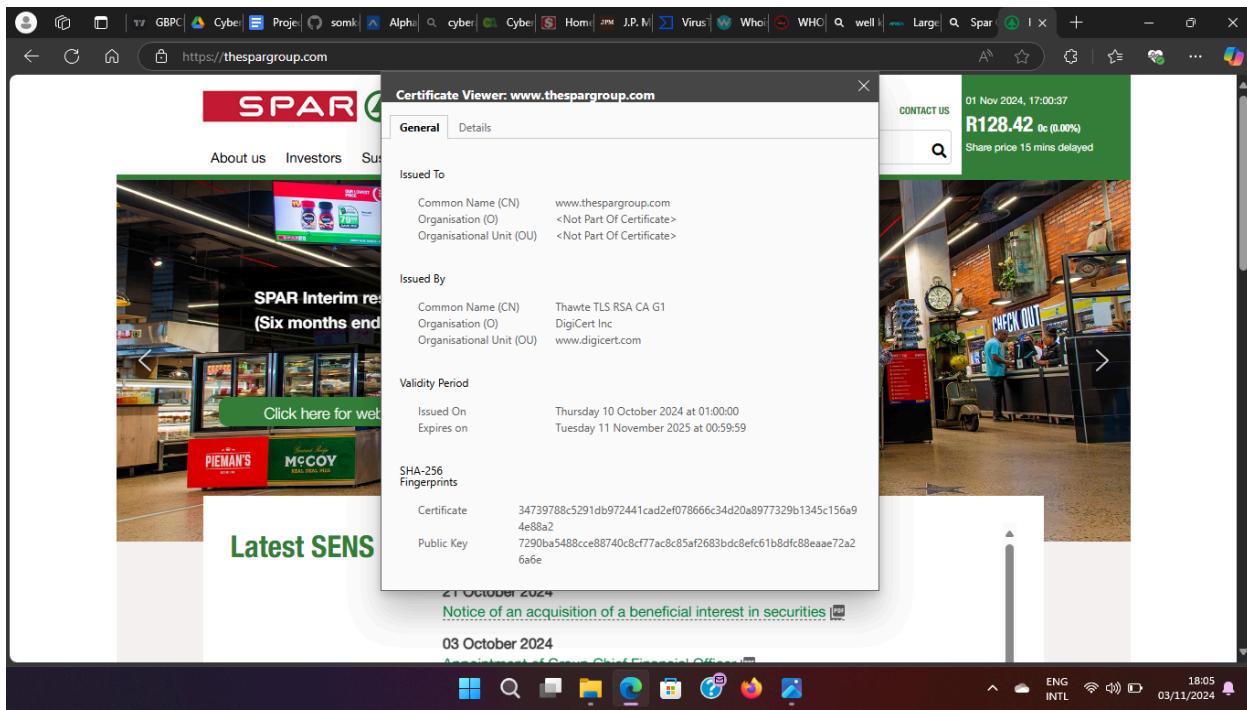
ISP	GMO Internet Group Inc.
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	v163-44-161-169.b00c.g.tyo1.static.cnode.io
Domain Name	gmo.jp
Country	Japan
City	Tokyo, Tokyo

IP info including ISP, Usage Type, and Location provided by IP2Location.  
Updated monthly.

At the bottom of the page are two buttons: "REPORT 163.44.161.169" and "WHOIS 163.44.161.169". The system tray at the bottom right shows the date and time as "03/11/2024 16:33".

The IP wasn't found in abuseipdb database, meaning that no report of malicious activities has been reported of it yet . Other details shows its correspondence with whoer.net

## B. Thespargroup.com

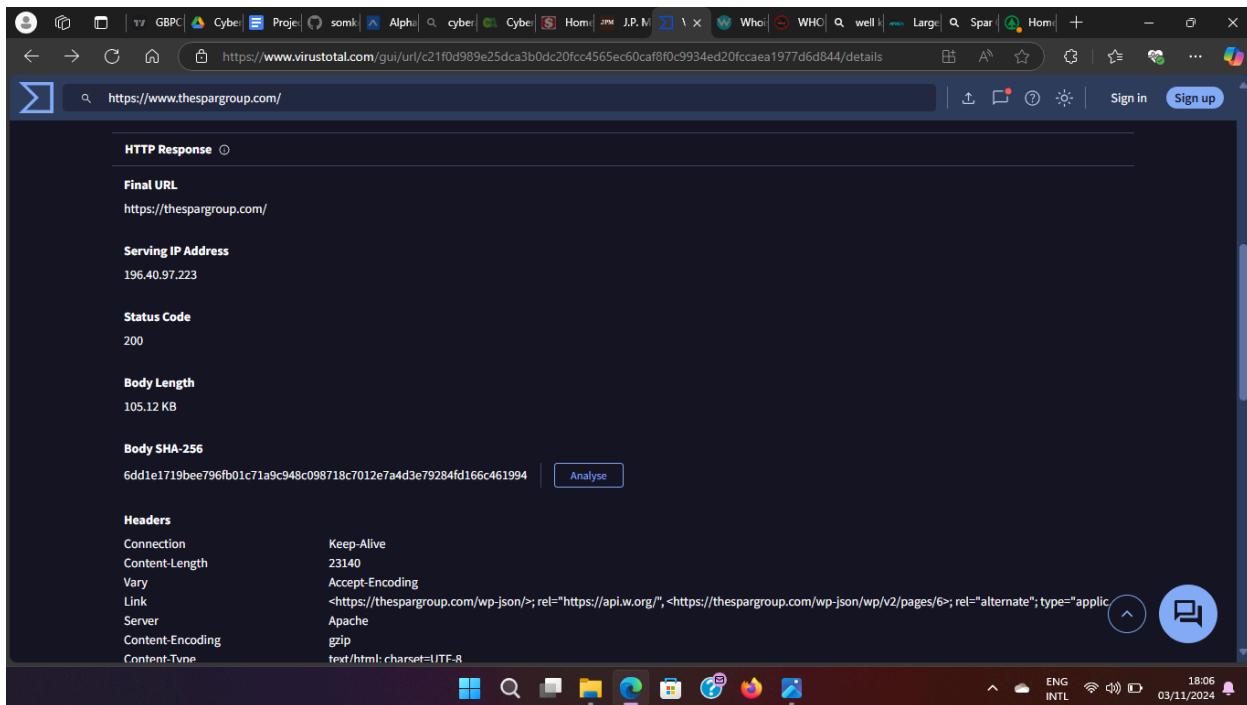


The screenshot shows a certificate viewer for the website [www.thespargroup.com](https://thespargroup.com). The interface includes a sidebar with the SPAR logo and a main panel for 'Certificate Viewer'. The 'General' tab is selected, displaying the following information:

- Issued To:** Common Name (CN): www.thespargroup.com; Organisation (O): <Not Part Of Certificate>; Organisational Unit (OU): <Not Part Of Certificate>
- Issued By:** Common Name (CN): Thawte TLS RSA CA G1; Organisation (O): DigiCert Inc; Organisational Unit (OU): www.digicert.com
- Validity Period:** Issued On: Thursday 10 October 2024 at 01:00:00; Expires on: Tuesday 11 November 2025 at 00:59:59
- SHA-256 Fingerprints:** Certificate: 34739788c5291db972441cad2ef078666c34d20a8977329b1345c156a94e88a2; Public Key: 7290ba5488cce88740c8cf77ac8c85af2683bdc8efc61b8dfc88eaee72a26ab6

A small thumbnail image of a supermarket interior is visible on the right side of the viewer.

An Overview of the certificate viewer, showing important details of the website



The screenshot shows the VirusTotal analysis page for the URL <https://www.thespargroup.com/>. The analysis results are as follows:

- HTTP Response:**
  - Final URL:** <https://www.thespargroup.com/>
  - Serving IP Address:** 196.40.97.223
  - Status Code:** 200
  - Body Length:** 105.12 KB
  - Body SHA-256:** 6dd1e1719bee796fb01c71a9c948c098718c7012e7a4d3e79284fd166c461994
- Headers:**

Header	Value
Connection	Keep-Alive
Content-Length	23140
Vary	Accept-Encoding
Link	< <a href="https://thespargroup.com/wp-json/">https://thespargroup.com/wp-json/</a> >;rel="https://api.w.org/",< <a href="https://thespargroup.com/wp-json/wp/v2/pages/6/">https://thespargroup.com/wp-json/wp/v2/pages/6/</a> >;rel="alternate";type="application/json"
Server	Apache
Content-Encoding	gzip
Content-Type	text/html; charset=UTF-8

The url was scanned on virustotal.com to reveal it's IP address (196.40.97.223)

Network: 196.40.96.0/20  
Autonomous System Number: 37153  
Autonomous System Label: xneelo  
Regional Internet Registry: AFRINIC  
Country: ZA  
Continent: AF

Last HTTPS Certificate

JARM Fingerprint: 2ad2ad0002ad2ad00042d42d000007d9a2df75fc17326c15d1e44e597e360

Last HTTPS Certificate

Data:

Version: V3  
Serial Number: d50a60954e1af6eb5775a00a5cf5949  
Thumbprint: ac2fbfb4c71fda38b940ef0cebbb3a1ce7f8f714

Signature Algorithm:

Issuer: C=US , O=DigiCert Inc , OU=www.digicert.com , CN=GeoTrust TLS RSA CA G1

Validity

Not Before: 2023-06-14 00:00:00  
Not After: 2024-07-09 23:59:59

Subject: CN=\*.cpt1.host-h.net  
Subject Public Key Info:

Public Key Algorithm : RSA  
Public-Key: (4096 bit)  
Modulus:

The IP address was further scanned, and its certificate details corresponded with the one seen on the certificate viewer

IP address: 196.40.97.223

Location: South Africa (ZA),N/A  
Region: N/A  
City: N/A  
ZIP: N/A

Hostname: dedi160.cpt1.host-h.net → 196.40.97.223  
IP range: 196.40.96.0 - 196.40.111.255  
ISP: xneelo  
Organization: xneelo

Blacklist: Yes ()  
TOR: No

Zone: Africa/Johannesburg  
Local: Sun Nov 3 2024 19:09:05 GMT+0200 (SAST)

Further scanning on whoer.net revealed more details of the domain including its geolocation (Johannesburg, SouthAfrica)

The screenshot shows a Microsoft Edge browser window with the URL <https://www.abuseipdb.com/check/196.40.97.223>. The page title is "AbuseIPDB » 196.40.97.223". A search bar at the top contains the text "e.g. 102.91.4.11, microsoft.com, or 5.188.10.0/24". An orange "CHECK" button is to the right. On the left, there's a "feedback" link. The main content area displays the following information for the IP address 196.40.97.223:

ISP	Xneelo (Pty) Ltd
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	dedi160.cpt1.host-h.net
Domain Name	xneelo.com
Country	South Africa
City	Cape Town, Western Cape

IP info including ISP, Usage Type, and Location provided by IP2Location.  
Updated monthly.

At the bottom are two buttons: "REPORT 196.40.97.223" and "WHOIS 196.40.97.223". The system tray at the bottom right shows the date as 03/11/2024 and the time as 18:10.

Scanning on abuseipdb showed the IP address has not been reported for any malicious activity

## C. Tesla.com

The screenshot shows a Microsoft Edge browser window with the URL <https://www.tesla.com>. A certificate viewer overlay is displayed in the center. The title of the overlay is "Certificate Viewer: \*.tesla.com". The "General" tab is selected. The details shown are:

Issued To	Common Name (CN): *.tesla.com Organisation (O): TESLA, INC. Organisational Unit (OU): <Not Part Of Certificate>
Issued By	Common Name (CN): GeoTrust RSA CA 2018 Organisation (O): DigiCert Inc. Organisational Unit (OU): www.digicert.com
Validity Period	Issued On: Monday 22 January 2024 at 01:00:00 Expires on: Thursday 23 January 2025 at 00:59:59
SHA-256 Fingerprints	Certificate: 6521ba26b971fd8b2ba1aee31fc2780d8061ad25742078f765ff4cddd46e0fbdf47b8c0d9906603e87d474f358ff4a6da8ded38215eda007ecf20d70977755bf Public Key: 75b9f

The background of the browser window shows a blurred image of a road through a forest.

An Overview of the certificate viewer, showing important details of tesla.com

The screenshot shows the VirusTotal analysis page for the URL <https://www.tesla.com/>. The analysis includes:

- Categories:** BitDefender, Xcitium Verdict Cloud, Sophos, Forcepoint ThreatSeeker. Verdicts: auto, motor vehicles, vehicles, vehicles.
- History:** First Submission: 2016-07-18 21:37:51 UTC; Last Submission: 2024-11-03 16:56:53 UTC; Last Analysis: 2024-11-03 16:56:53 UTC.
- HTTP Response:** Final URL: <https://www.tesla.com/>.
- Serving IP Address:** 23.206.160.45.
- HTML Info:** Trackers: Google Tag Manager, Bing Ads.

The url was scanned on virustotal.com to reveal its IP address (23.206.160.45)

The screenshot shows the VirusTotal analysis page for the IP address 23.206.160.45. The analysis includes:

- Last HTTPS Certificate:** JARM Fingerprint: 2ad2ad0002ad2ad00042d42d000000d71691dd6844b6fa08f9c5c2b4b882cc.
- Last HTTPS Certificate Data:** Version: V3, Serial Number: af2e42f96babd99739d56cecb587665, Thumbprint: 0ffe7a88524ee668e3b677c9a32083e0f3787e59.
- Signature Algorithm:** Issuer: C=US , O=DigiCert Inc , OU=www.digicert.com , CN=GeoTrust RSA CA 2018.
- Validity:** Not Before: 2024-01-22 00:00:00, Not After: 2025-01-22 23:59:59.
- Subject:** C=US , ST=Texas , L=Austin , O=TESLA, INC. , CN=\*.tesla.com.
- Subject Public Key Info:** Public Key Algorithm : RSA, Public-Key: (2048 bit), Modulus: b5:ef:17:12:e5:94:75:96:99:06:01:6d:c6:81:fc: 4b:1f:9d:e4:dc:8d:f1:59:69:29:f6:f0:0e:3b:6a: 25:a6:1f:60:f8:91:68:ec:ed:55:1f:3e:d9:87:fb: 15:4f:ad:9d:id:4e:bf:40:a7:21:d6:27:c1:c5:6f: f5:49:20:8e:06:ec:41:73:fd:7b:a5:7f:e4:a2:65.

The IP address was further scanned and the certificate details corresponded with that seen on the website's certificate viewer

The screenshot shows a web browser window with the URL <https://whoer.net/checkwhois>. The page is titled "WHOER" and features a navigation bar with links for "My IP", "VPN", "Download", "Antidetect Browser", "AML check", "Services", "Hide my data", and "Help". A red button on the right says "Grab -75% Now". The main content area displays the IP address **23.206.160.45**. Below it, two columns of information are shown:

Location:	United States (US), N/A
Region:	Texas (4736286)
City:	Dallas
ZIP:	75270
Hostname:	a23-206-160-
	45.deploy.static.akamaitechnologies.com →
IP range:	23.206.160.45
ISP:	Akamai Technologies
Organization:	Akamai Technologies
Blacklist:	<a href="#">Yes ()</a>
TOR:	No
Zone:	America/Chicago
Local:	Sun Nov 3 2024 11:25:56 GMT-0600 (CST)

The bottom of the screen shows a taskbar with various icons and a system tray indicating the date and time as 03/11/2024 at 18:26.

Further scanning on whoer.net revealed more details about the IP address including its geolocation (Texas, U.S.A)

Check an IP Address, Domain Name, or Subnet  
e.g. 102.91.4.11, microsoft.com, or 5.188.10.0/24

102.91.4.11 **CHECK**

**23.206.160.45 was not found in our database**

ISP Akamai Technologies Inc.

Usage Type Content Delivery Network

Hostname(s) a23-206-160-45.deploy.static.akamaitechnologies.com

Domain Name akamai.com

Country United States of America

City Dallas, Texas

IP info including ISP, Usage Type, and Location provided by IP2Location.  
Updated monthly.

REPORT 23.206.160.45 WHOIS 23.206.160.45

The IP address wasn't found on abuseipdb indicating that its hasn't been reported for any malicious activity or attempt

## RECOMMENDATION

1. The respective organizations should endeavor to renew their certificates as and when due.
2. The cryptographic algorithms used in securing the domains should be evaluated and updated continually to ensure maximum data encryption.
3. Additional security measures like multi-factor authentication, Intrusion Detection and Prevention systems should not be left out for further strengthening of data protection.

## CONCLUSION

In conclusion, the analysis results show a high confidence in the domain authenticity respectively and therefore are safe to interact with. However, Subsequent and deeper analysis can be done as well to prevent any vulnerability that could lead to potential cyberattacks ranging from certificate spoofing, Certificate authority compromise , etc