Multi-Factor Authentication Project

Presented by Celestine A. Ugwu, to

HALOGEN GROUP / FEDERAL MINISTRY OF YOUTH AND SPORTS DEVELOPMENT

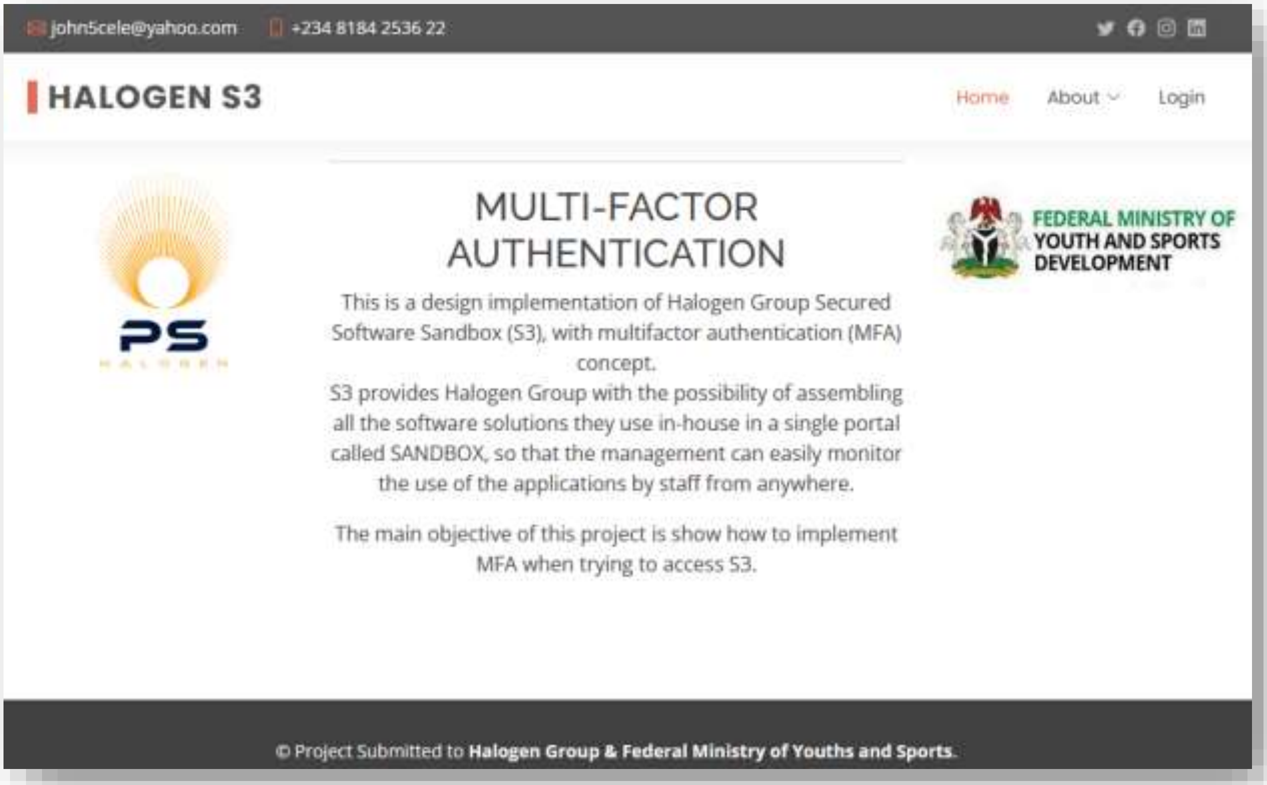
November 28, 2022.

Abstract

It is no longer news that cyber-attack is on the rise as more than 80% of global businesses have been predicted to be on cloud in the nearest future. This necessitates the inevitable need to strengthen the fortress of our online and offline software applications. Among the many practices already on ground to mitigate the impending doom, multiple factor authentication (MFA) has become the most prevalent and successful approach to sign on to any cloud-based application with minimal cases of successful attack. MFA uses, at least, more than one method of authentication to verify the authenticity of users.

MFA is popular because of its excellent features of combining what the user knows, and/or what the user possesses. User must know his username and password, as well as, having his phone or electronic device with him to access any message that could be sent to him to finally authenticate himself as the genuine user of the application.

In this project, I have been able combine username and password with basic active directory policy to authenticate users; and then a bit of AI approach to determine if the user should be subjected to MFA or not. When the need abounds, the user would be required to access a secret code sent to his phone number or email address to finally get authenticated before a successful logon would be granted.
The authentication procedures of this project considered user credentials, the location of login, the device in use, the operating system of the device, the ISP connected to, the browser in use, and the number of inactions in days.



johnScele@yahoo.com +234 8184 2536 22

HALOGEN S3

Home About Login

PS HALOGEN

MULTI-FACTOR AUTHENTICATION

This is a design implementation of Halogen Group Secured Software Sandbox (S3), with multifactor authentication (MFA) concept.
S3 provides Halogen Group with the possibility of assembling all the software solutions they use in-house in a single portal called SANDBOX, so that the management can easily monitor the use of the applications by staff from anywhere.

The main objective of this project is show how to implement MFA when trying to access S3.

FEDERAL MINISTRY OF YOUTH AND SPORTS DEVELOPMENT

© Project Submitted to **Halogen Group & Federal Ministry of Youths and Sports.**

1.0 Introduction

As a matter ingenuity, the developmental cycle of this software solution took about three weeks to touch the entire phases ranging from conceptualization, design and code implementations; meanwhile, the key purpose is to develop useful software with main focus on the multifactor authentication (MFA) which will guarantee error-free and user-friendly web-based application that will require multiple authentication phases to get logged on to the server without any security compromise.

This piece of document explains, in various steps, the software solution itself, and the MFA stages integrated to ensure zero attack. The conclusion discusses the limitations and recommendations required for a complete package to fit into any business environment such as public and private companies, and also perfect for government institutions.

2.0 MFA as related to Secured Software SandBox (S3)?

S3 is the actual software solution developed, the MFA remains the authentication pattern integrated into the software application for security purposes.

2.1 MFA

MFA is an acronym for Multi-factor Authentication. It is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack. (https://www.onelogin.com/learn/what-is-mfa, 2022).

2.2 Secured Software SandBox (S3)

S3 stands for Secured Software Sandbox. It is a concept that delved into my head after registering for the Halogen cyber security challenge award in November 2022; the principal aim of S3 is to organize all Halogen software solutions into a common and simple portal, herein referred to as sandbox, to enable easy usage and monitoring from cyber-attacks.

The idea of S3 is to help Halogen management to manage and monitor the use of their software from anywhere. S3 can keep track of:

- Who did run the software
  S3 keeps a log of all users logging into Halogen portal (sandbox); and user name validation is the very first action before even getting access into the software.
- When did he log in
- Where (Location) did he log in from
- Which device did he use to log in
- Which browser did he use, etc.

So, in the event of cyber-attack, the above information will be of great help in developing a critical and info-based forensic research on the cause(s) of the attack, as well as, the basis for mediation.

3.0 MFA Implementations

This describes the various programming implementations of MFA in order to access S3 on server. The first stage is to get registered to use the application, as herein captured as pre-registration, and then followed by a login, with its accompanying checks and validations as explained in the following subsections.

3.1 Pre-Registration

The software solution herein referred to as S3 is an internal utility application, which implies that you must be a bona-fide staff of the Halogen Group before you can even be admitted into using it. So, the home page of S3 is available to everyone, but you can only use a pre-registration link to inform the Halogen management of your interest in using S3. After pre-registration, an email message will be sent to the management for proper assessment, after which you would be got back to, either approved or declined. If approved, the initial credentials provided by the applicant at the time of pre-registration would be forwarded to him for the first login to enable him change his/her password. It is also possible to register users directly by Halogen high role personnel without passing through pre-registration process.

3.2 Login

When a user must have acquired valid username and password, he can now use it to login at https://halogen.veracelservers.com. Veracelservers.com is a domain name registered by me for the purpose of web application testing. I simply created a sub-domain called halogen for this exercise.

Testing on a valid server is sacrosanct as it is difficult to implement email notifications without internet connections to the client devices; however, this application can run completely offline but with the limitation of email and SMS notification services which all depend on internet connection. For users to login, an AI background checks are done to ascertain if the user should be subjected to MFA or direct login using only username and passwords.

3.2.1 Authentication (MFA) Login

When a user enters his username and password in the login page, the following AI checks are carried out in the background. These are checks are, and not limited to username acceptance, password checks, last visit queries such as time, location, device used, browser used, etc.

3.2.1.1 Username Acceptance

S3 accepts your username if it is found in the database, and its status is valid.

3.2.1.2 Password Check

It checks if your username and password are correct, if true, then the checks for last login information are sought.

3.2.1.3 Last Time Visit

If you pass the username and passwords checks, S3 checks the last time you logged on to server. There is a preset number of hours that if one fails to visit the server, one would be required to be validated by MFA. If the returning user satisfies this, then the AI actuates the last location query.

3.2.1.4 Login Location Change

S3 checks the location of LAST login; if it is the same location as the current location, then it will shift to the next query. This is achieved by checking the internet modem and the IP used in the previous logon. Note that this feature can be perfected only when we partner with the ISP companies so as to accurately capture the base station closest to the S3 users. For now, if the user changes an internet modem from MTN to GLO while still on same chair, S3 will sense a change of location and flag an MFA.

3.2.1.5 Browser Switch Intelligence

S3 checks the last browser used in the previous logon. If an S3 user switches internet browser, that is, changing from Firefox to Chrome, or others, MFA will be triggered.

3.2.1.6 Gadget / Machine Switch

S3 compares the current gadget with the previous one; for example: if you logged on previously from PC, and you are logging in now with phone, MFA will be triggered. MFA will also trigger when you want to use same PC with a different account; or even trying to login in from another user's PC with different OS. Any time you try to login with phone or tablet for the first time after previously logging on with PC, MFA would be triggered; however, if you continue with the same phone or tablet, you will be forced to MFA assuming all other conditions are met. But any attempt to user another phone different from the regular one you use; MFA will surely trigger.

3.2.2 Direct Login

When all the conditions as enumerated in item(s) 3.2.1 are not the case, then the users can log on with their usernames and passwords only without further authentications. This is eminent to avoid incessant authentications during any daily routine assignments; however, users are automatically logged out when their browsers observe INACTIVITY for about twenty minutes. This is to ensure that intruders do not impersonate them when they are not around their computer systems, especially when they are on break.

3.2.3 MFA Methods Applied.

As the name implied, MFA uses more than, at least, one authentication method to verify that the user is the right person.
For S3, I implemented three different ways of ensuring that imposters do not have access to S3 server. Combinations of password, email and phone SMS are used.

3.2.3.1 Username and password

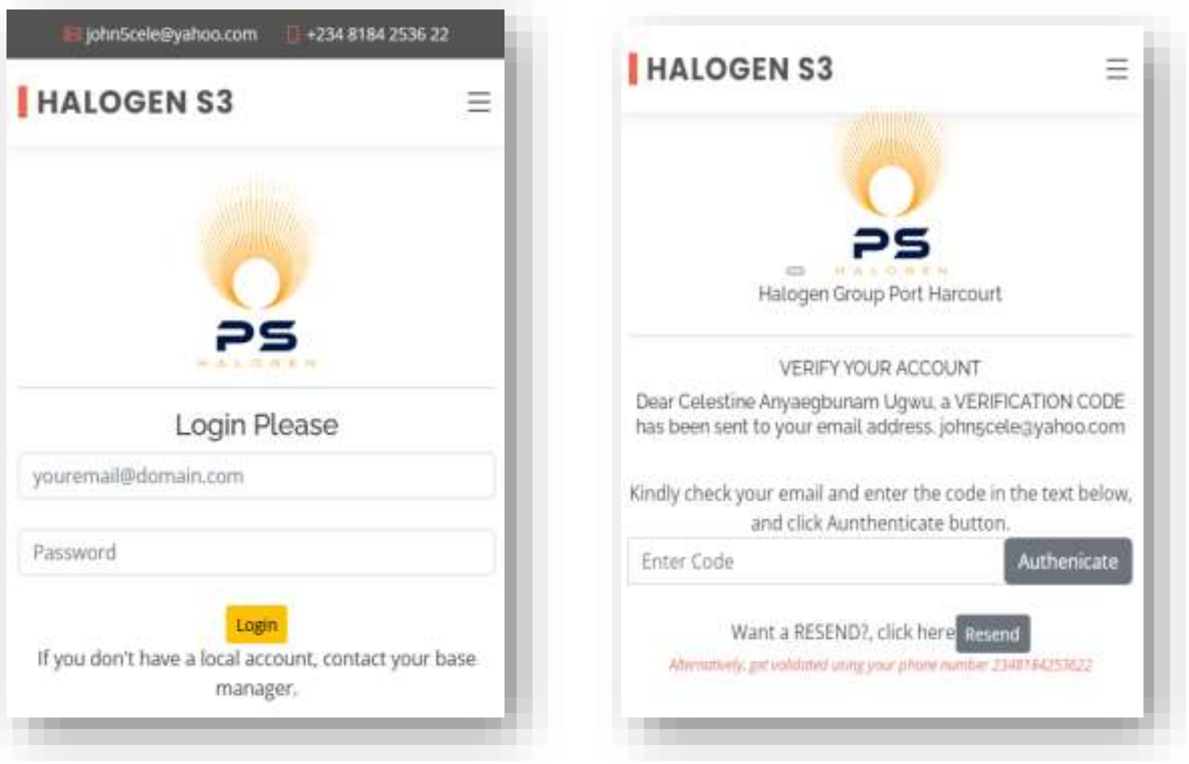
Your username must be valid, and password must be correct before you qualify to the next login stage.

3.2.3.2 Email Address.

A verification code is sent to your registered email address. In addition, you must use the code within a preset number of minutes unless it expires.
be correct, verification code is sent to your registered email address with a sender ID mfa.halogen@veracelservers.com or mfa@veracelservers.com as both have been created on the email server for this purpose.

3.2.3.3 Phone SMS

You are provided with an alternative of receiving a verification code in your registered SIM number. When this option is chosen, the user would receive an SMS message with “HALOGEN “as a sender ID, and 5–6-digit secret codes as the message body.



john5cele@yahoo.com +234 8184 2536 22

HALOGEN S3

Login Please

youremail@domain.com

Password

Login

If you don't have a local account, contact your base manager.

HALOGEN S3

Halogen Group Port Harcourt

VERIFY YOUR ACCOUNT

Dear Celestine Anyaegbunam Ugwu, a VERIFICATION CODE has been sent to your email address. john5cele@yahoo.com

Kindly check your email and enter the code in the text below, and click Aunthenticate button.

Enter Code

Authenicate

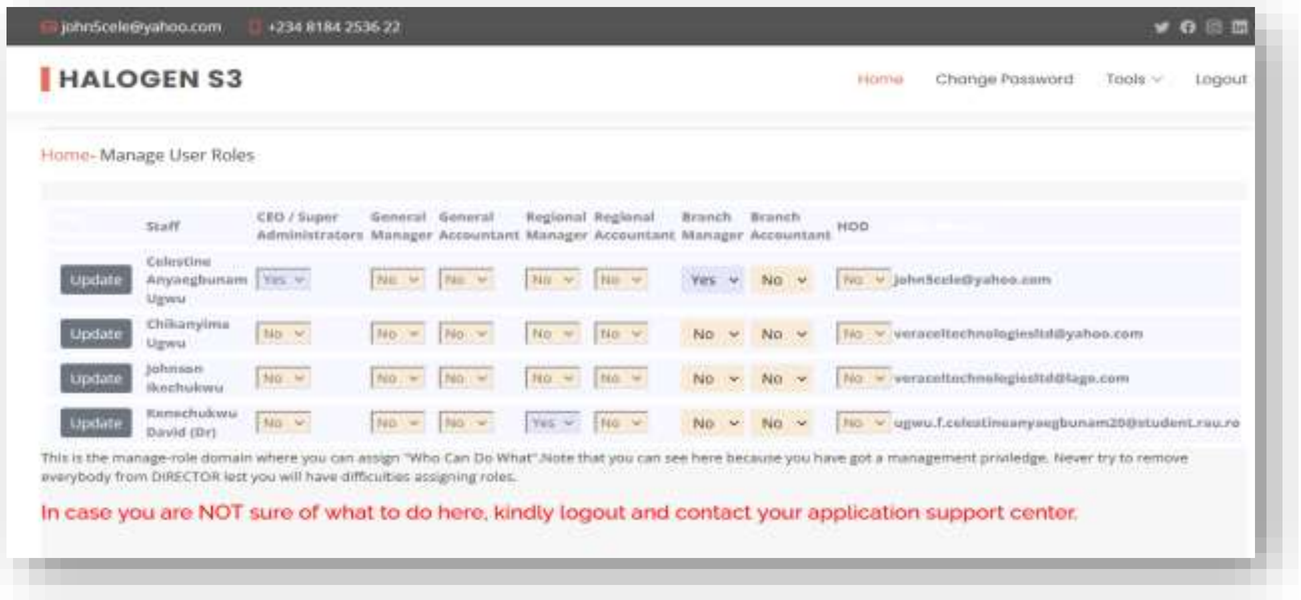
Want a RESEND?, click here Resend

Alternatively, get validated using your phone number 2348184253622

Figure 3.0 Login and Account Authentication Environment

3.2.3.4 Role Management and Activity Log System

This is not part of MFA, but this enables the Halogen management to keep track of all login attempts from users. Also, in the S3, all users are categorized into different roles ranging from Director, general manager, regional manager, branch manager, etc. As a director, you can access all regions and branches of Halogen Group; while regional managers can only access all branch offices within their respective regions; and branch managers can only access their specific branch applications and users.



john5cele@yahoo.com +234 8184 2536 22

HALOGEN S3

Home- Manage User Roles

	Staff	CEO / Super Administrators	General Manager	General Accountant	Regional Manager	Regional Accountant	Branch Manager	Branch Accountant	HOD	
Update	Celestine Anyaegbunam Ugwu	Yes	No	No	No	No	Yes	No	No	john5cele@yahoo.com
Update	Chikanyima Ugwu	No	No	No	No	No	No	No	No	veraceltechnologiesltd@yahoo.com
Update	Johnson Ikechukwu	No	No	No	No	No	No	No	No	veraceltechnologiesltd@lago.com
Update	Kenechukwu David (Dr)	No	No	No	Yes	No	No	No	No	ugwu.f.celestineanyaegbunam20@student.rau.ro

This is the manage-role domain where you can assign "Who Can Do What".Note that you can see here because you have got a management prinledge. Never try to remove everybody from DIRECTOR lest you will have difficulties assigning roles.

In case you are NOT sure of what to do here, kindly logout and contact your application support center.

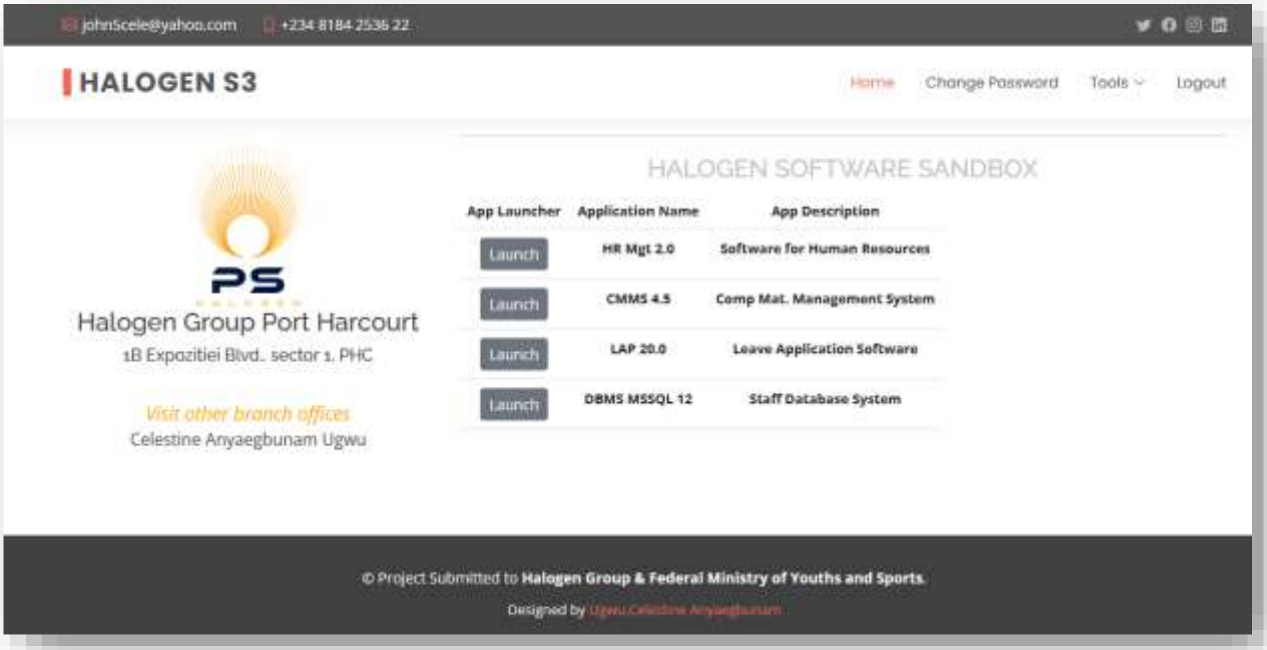
4.0 Secure Software SandBox (S3)

S3 stands for Secured Software Sandbox. It is a concept that delved into my head after registering for the Halogen cyber security challenge award; the principal aim of S3 is to organize all Halogen software solutions into a common and simple portal, herein referred to as sandbox, to enable easy usage and monitoring from cyber-attacks.

The idea of S3 is to help Halogen management to manage and monitor the use of their software from anywhere. S3 can keep track of:

- Who did run the software
  S3 keeps a log of all users logging into Halogen portal (sandbox); and user name validation is the very first action before even getting access into the software.
- When did he log in
- Where (Location) did he log in from
- Which device did he use to log in
- Which browser did he use, etc.

So, in the event of cyber-attack, the above information will be of great help in developing a critical and info-based forensic research on the cause(s) of the attack, as well as, the basis for mediation.



johnScele@yahoo.com +234 8184 2536 22

HALOGEN SOFTWARE SANDBOX

App Launcher	Application Name	App Description
Launch	HR Mgt 2.0	Software for Human Resources
Launch	CMMS 4.5	Comp Mat. Management System
Launch	LAP 20.0	Leave Application Software
Launch	DBMS MSSQL 12	Staff Database System

Halogen Group Port Harcourt
1B Expozitiei Blvd., sector 1, PHC

Visit other branch offices
Celestine Anyaegbunam Ugwu

© Project Submitted to **Halogen Group & Federal Ministry of Youths and Sports.**
Designed by Ugwu.Celestine Anyaegbunam

Figure 4.0 S3 Home

5.0 Conclusion/ Recommendations

Coming soon…

References

https://www.onelogin.com/learn/what-is-mfa. (2022, November 27). Retrieved from https://www.onelogin.com: https://www.onelogin.com/learn/what-is-mfa