I. J. Computer Network and Information Security, **2018, 1, 36-43**
Published Online January 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.01.05

Application of Geo-Location-Based Access Control in an Enterprise Environment

Victor L. Yisa
Federal University of Technology, Minna/ Department of Cybersecurity Science, 920001, Nigeria
Email: victor.yisa@futminna.edu.ng

Baba Meshach[2], Oluwafemi Osho[3] and Anthony Sule[4]
Department of Cybersecurity Science Federal University of Technology, Minna, 920001, Nigeria
Email: {babameshach01[2], femi.osho[3]}@futminna.edu.ng, Anthonysule39@gmail.com[4]

Received: 04 July 2017; Accepted: 02 November 2017; Published: 08 January 2018

***Abstract*—**Unauthorized Access has been difficult to stop or prevent in the last few decades using username and password authentication only. For an individual, data breach might just be a simple case of espionage or the loss of private credentials, for an enterprise, this could mean the loss of billions of dollars. Preventing Unauthorized Access to Enterprise Systems Using a Location-based Logical Access Control proposes a framework that uses time and location in preventing and defending against data breaches. The framework was developed using Java with an Eclipse IDE. The database was designed using MySQL and locations were collected using Google Maps API. Users registered at different locations in a university campus were unable to access another's account in the database because they were both outside the known location and tried to do this at off-work hours. Users were registered with username and password at specified locations. The users are then made to login from same and different locations with correct username and passwords. it was discovered that access to the database was only given when the username and password was correct and location was same as at registered or as allowed by an administrator. The system was found to protect against unauthorized access arising from stolen login credentials and unauthorized remote logins from malicious users.

***Index Terms*—**Unauthorized Access, Access control, geolocation, Administrator, Google Gears, Location.

I. INTRODUCTION

Over the years, the need for security of data and information resources has heightened (Bertolissi & Fernández, 2008) [1]. One of the greatest concerns in any enterprise environment is unauthorized access to its data and other information resources. Unauthorized access, whether into personal or corporate files and asset, as we know it today is a term which characterizes the actual act of gaining access into a property without the required permissions. An attacker targeting an enterprise environment would usually try to compromise one or more of the 3 P's: people, password, and physical security.

Password is the most popular gateway to gaining access to many networks. When an attacker hacks the password of a legitimate user, often remotely, he gains access to the network. There are many attacks, involving both technical and non-technical procedures, which an attacker could launch to 'steal' passwords. These include phishing, social engineering, password guessing, sniffing, eavesdropping, and man-in-the-middle attacks.

People have often been deemed the most vulnerable of the three. Apart from their susceptibility to attacks like social engineering and phishing, they frequently fall short of adhering to security measures applicable in their enterprise. For instance, a user saves his password(s) on the computer, such that the system remembers his password each time he tries log in to any service. If the physical security mechanisms in place are not adequate, an attacker could steal such system. Consequently, unauthorized access is gained by the attacker to the services on the enterprise network. This problem becomes aggravated if the user is an administrative user.

The traditional approach to access control employs the use of authentication mechanism often in the form of username and passwords to verify access requests [2][3]. Some of the shortcomings associated with this mechanism are exposed by the above examples. However, one possible method of ensuring that an attacker who obtains the password or gains physical access to the system of an employee does not access the enterprise's network is via the use of location awareness information, in addition to the traditional authentication methods[4]. Attackers are very likely to experience difficulties in their bid to compromise a system grounded together with its users, to a particular location[5]. Knowing, for instance, that an employee is expected to be in the office within specific time duration, access packets from a remote location, using stolen authentication details of the employee, would not be permitted. In the same vein, an attacker who removes an employee's system to another location would not be able to access any service on the network of the enterprise, since the system would have been configured to access only from its original position.

Application of location-based information has already found its place in smartphones[6][7], social networking, electronic finance [8], and fraud detection[9]. However, in reality, using geographical location (rather than just knowledge, possession and biometrics) for authentication, relatively, is a new direction in the field of information security [10], and thus only a few in-depth designs and methodologies have been done on the subject matter.

In this study we develop a geo-location-based access control mechanism, applicable in an enterprise environment, for preventing unauthorized access to its database. Essentially, to achieve this objective, we develop a test database, to serve as the object to be protected; implement a geo-location API that automatically detects and collects a user's location; and develop a web application that incorporates the API to secure the database.

This study is organized as follows: section I discuss the existing location determining mechanisms; the concept of geo-location is reviewed; discussion on Google gears. Section II is related works while The Methodology is in section III. Section IV and V is the discussion of result and conclusion respectively

A. *Existing Location Determining Mechanisms*

Different forms of complex security technologies such as end-point management, data encryption, and network access control such as firewalls are use in protecting our data against illegal access. But these technologies can be rendered in-effective if an attacker can provide valid login credentials, which they can obtain through phishing, social engineering, keystroke capture, default password, password cracking and stolen password.

Two factor authentication (TFA) is now been implemented to make authentication into a device /system more secure. Multi-factor authentication is regarded as the most secure means of securing our data, as the attacker needs to pass through two or more forms of authentication before been granted access. Multi-factor authentication was created to address the challenges of single factor authentication. Most two factors authentication combine "what you know" such as password and "what you have" such as token and mobile devices.

One of the most common two factor authentications is SMS-Based. SMS is sent to a mobile device which is then typed in by the user. SMS-Based authentication is gradually been deprecated [11]. The drawbacks of this method of authentication are (1) the device can be misplaced or stolen, (2) poor network service can affect the time of message delivery (3) the messages which can be view through desktop can easily be compromised if the desktop is compromised.

Another similar form of authentication involved installation of an application on mobile device that makes use of time-based one time password algorithm. A good example of this is Google authenticator. Google authenticator uses hash of the known and shared secret key between the server and the mobile application to generate the one time password. This method has a similar drawback to that of sms based as device can also be misplaced and the user needs to type in google authentication password which may not be convenient for the users [12]. The OTP expiration is between 1 minute to an hour depending on the service provider. This large expiration time is good enough for the attacker to compromise the system.

Zero-interaction authentication (ZIA) is a mechanism of authentication into a system using an authenticating token (e.g., a wristband, a Smartphone) in close proximity with the system. ZIA has a very good usability as the user does not need to memorize nor type in password. ZIA can be vulnerable to replay attack because it makes use of some constant network component such as MAC address. It can also be stolen, granting the unauthorized user unfettered access to the terminal [12].

[13] Designed another form of authenticating system that makes use of a femtocell placed at a specified location. Any ingress traffic activity passing through any mobile device associated with femtocell can verify the mobile receiver's location based on femtocell.

B. *Geolocation*

It is a technique use in estimating the geographical location of a person or an object through the use different positioning systems and algorithm [14]. Location tracking and positioning systems uses different techniques to sense and measure the location of a mobile device at any given time. The techniques use in tracking the location of a device can be grouped into four namely:

i. Cell of origin (*nearest cell*)
ii. Distance (*lateration*)
iii. Angle (*angulation*)
iv. Location patterning *(pattern recognition)*

The combination of two or more of these techniques can be use in eliminating the weaknesses found within individual techniques to achieve a better result and performance in different environment. The accuracy of real time location of an object at any particular point in time depends mostly on current timestamps, angle of incidence measurement, probe responses, polling interval of the server and the signal strength readings [15]

Geolocation: It is a technique use in estimating the geographical location of a person or an object through the use different positioning systems and algorithm. The location and accuracy radius of Google Maps Geolocation API is based on the information it collects and analyzed from cell towers and WiFi nodes of the mobile clients (Geolocation API, June 2017)). It does not require GPS to work properly as it constantly updates its database through crowd sourcing from billions of android phones, WiFi points and Cell IDs around the world. Its advanced positioning algorithm enables it to have an accuracy of 10-20 meters or can be exact depending on how much data have been collected from that location. It also works well in both indoor and urban areas where

GPS normally struggles to refraction and obstruction to line of sight.

Geolocation has a lot of application in the area of cybersecurity, cyber attacks threatening to cause havoc on a facility can be stopped, and the attacker can be traced as using geolocation can help in providing the geographical information of the attacking host. Geolocation is also being used for fraud prevention by various financial platforms as these platforms are constantly susceptible to phishing attempts and other malicious schemes [17].

C. Gears

Gears (Google Gears) was software developed by Google to support powerful web applications through new features it adds to web browsers. Gears is an open source set of java script API's that can be added to a browser and called from web applications [12]. Gears was discontinued in 2010 but can be enabled through greasemonkey user script on unsupported websites. Gears use a term called Geocoding which is a way of converting or transforming the address of a location, point of interest, systems or mobile devices into a geographic coordinates of latitudes and longitude on the earth surface [18].

The major API components of Gears are:

i. SQLite Database module with capability of storing data locally
ii. A WorkerPool module for parallel execution of JavaScript code.
iii. A LocalServer module, for caching and serving application resources
iv. A Desktop module
v. A Geolocation module, for geographical location detection of their users.

II. Related Works

Location-based access control (LBAC) has been suggested as a means to improve IT security. By restricting legitimate users to a defined location, attackers will find it more difficult to successfully compromise a system. [19] in their work Looked at a breakdown of the relationships in an LBAC; ionizing them into IT, Physical, Social and Legal contexts. Using geographical location (rather than just knowledge, possession and biometrics) for data authentication is a relatively new approach towards information security, [20] and thus only a few in-depth designs and methodologies have been done on the subject matter.

[21] Expressed locations as geometric n- dimensional coordinates, symbols or as a hybrid and implemented authentication using geostationary satellites or infrared sensors placed at strategic locations in the building where access control is required.

Aside the traditional means, preventing unauthorized access can be done by the use of biometrics. [22] Implemented an iris biometric system for security systems, while [23] proposed an e-voting system that would make use of fingerprint in ensuring authentication, integrity and confidentiality of the system.

III. Methodology

To achieve the aim of this project, the information system design methodology is adopted. This is composed in a four-stage development life-cycle, namely planning, analysis, design, and implementation [24]. An analysis of existing systems has been presented in the literature review section. Hence, this section essentially focuses on the analysis design of the system and provides information on the implementation process.

The design phase details the mechanism of operation (input, output, processing, and storage) of the system. In other words, it outlines how the infrastructure (hardware, software, and network), and the supporting necessities, including databases, files, user interface, forms, are interconnected. The design phase incorporates, but not limited to, the architecture design (which describes the hardware, software, and network infrastructure that will be used), interface design, and program design

A. Definition of Requirements of Proposed System

To overcome these challenges, this project introduces two, universal factor in checking authentication: Time and Location, which are jointly unique to every corporate environment and essential in controlling and defending against intruders/hackers. due to the shortcomings identified in the existing systems as discussed in the literature, the proposed system should be able to address the problems of hacking into a server/database by spoofing the IP address of the target system, it should also be able to address cases of identity theft where a genuine users credentials are stolen and used by a malicious user by just logging into the server.

Functional Requirements

i. The system must be able to verify correct login credentials to an access database
ii. The system must be able to accept a log on attempt if the username and password as well coordinates matches
iii. The system must be able to reject a log on attempt if the username and password is correct but the location coordinate doesn't match that set in the database
iv. A correct login will only be granted access if it is done during working hours as set by the administrator

Non-Functional Requirements

The non-functional requirements include:

i. Ease of use: the application should be designed in such a way that users will not find it complicating but easy to use
ii. Security: the system should ensure security of users respective accounts, a correct username and password may not be permitted if the location doesn't match as specified earlier during

registration and the administrator. also security is ensured and a user from a right location and correct login credentials might need a special permission from the administrator if the time of login doesn't tally has specified as allowable working periods.

Software Requirements
The software requirement are listed viz:

i. Windows Vista (and above)
ii. Eclipse Luna (Eclipse Kepler is also a good alternative)
iii. MySQL Server
iv. MySQL GUI
v. Apache Tomcat server (version 7.0 and above)
vi. Java Runtime Environment (jre 1.8.0_45)
vii. Web browser
viii. Google App Engine
ix. A Gmail account (For administrator)

B. Architecture of Proposed System

The framework was developed using Java with an Eclipse IDE. The database was designed using MySQL and locations were collected using Google Gears.

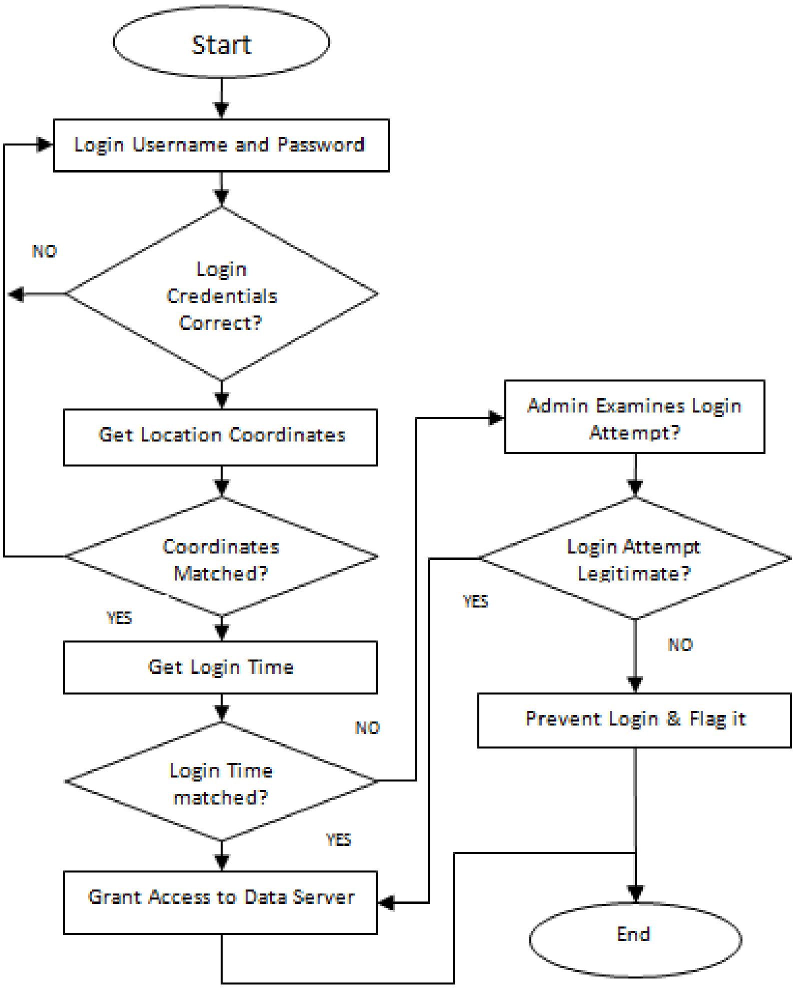

Start
Login Username and Password
NO
Login Credentials Correct?
Get Location Coordinates
Coordinates Matched?
YES
Get Login Time
NO
Login Time matched?
YES
Grant Access to Data Server
Admin Examines Login Attempt?
Login Attempt Legitimate?
YES
NO
Prevent Login & Flag it
End

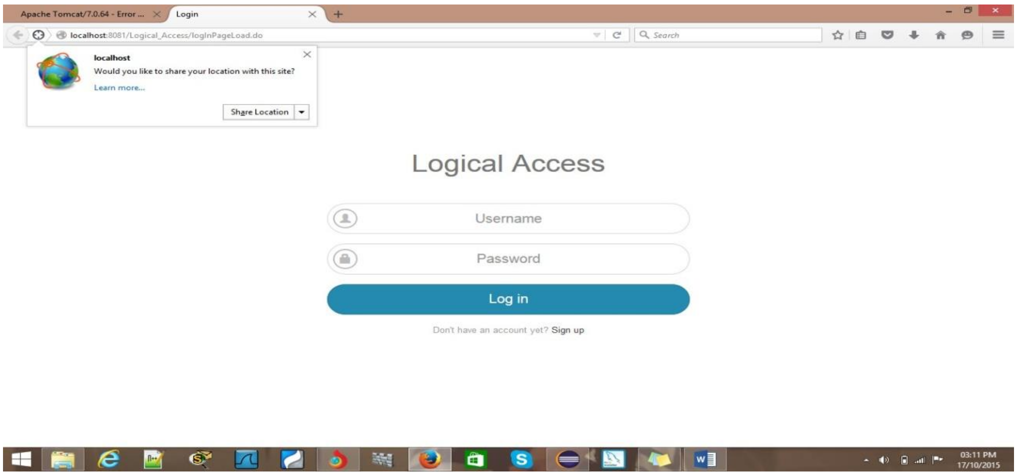
Fig.1. Flow Diagram for the Geo-location Access Control System

The flow process of the system is represent in the figure 1 above and is further explained below

i. The account holder identifies himself to the online account by providing username and password
ii. The system accepts or rejects the username or password as the case may be
iii. the user/accountholder then provides his present location to the system
iv. the system checks the location coordinates and see if it is permissible,
v. if the location is permitted, the system then checks if the attempted login time is permissible to the user
vi. if it is a permissible time then access is granted, otherwise the admin will ever to examine the user to know if he is to permit or not
vii. the user is then granted access to the system

C. *Results*

A new user is required to register during which his/her credentials such as name, sex, email, phone numbers, security questions are obtained, after which the users systems coordinates are obtained and stored. This login credentials and the coordinates must match for login to the enterprise servers to be successful. a registered user provides a correct username and password and is then required share the location of his/her computer, in case the coordinates obtained from the PC being used to login doesn't correspond with the registered coordinate associated with the account, access is denied. if the login credentials matches as well as the physical coordinates of the system, then the system checks if it is working hours, if it is not working hours, the system automatically contacts an administrator who can then permit or reject a login. A representation of the system login page is shown in the figure 2.



Apache Tomcat/7.0.64 - Error ... | Login

localhost:8081/Logical_Access/logInPageLoad.do

localhost
Would you like to share your location with this site?
Learn more...
Share Location

Logical Access

Username

Password

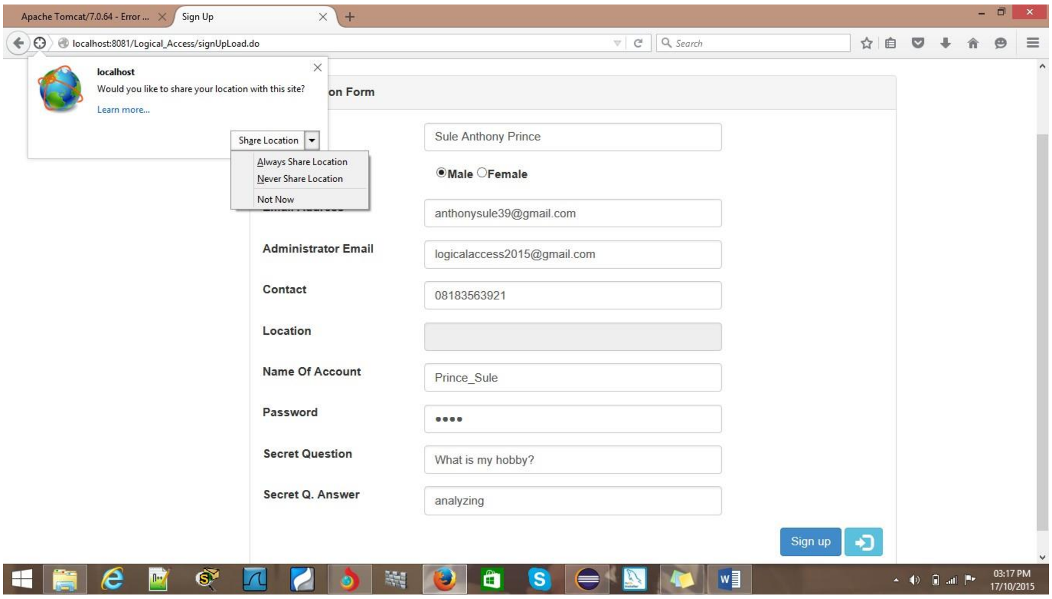
Log in

Don't have an account yet? Sign up

03:11 PM 17/10/2015

Fig.2. Login Page for the System

It shows the framework running on a Firefox web browser, its front end. A registered user can proceed to login with his username and password while the application verifies his location, for a first-time user however, he or she must first register.



Apache Tomcat/7.0.64 - Error ... | Sign Up

localhost:8081/Logical_Access/signUpLoad.do

localhost
Would you like to share your location with this site?
Learn more...
Share Location
Always Share Location
Never Share Location
Not Now

on Form

	Sule Anthony Prince
	● Male ○ Female
	anthonysule39@gmail.com
Administrator Email	logicalaccess2015@gmail.com
Contact	08183563921
Location	
Name Of Account	Prince_Sule
Password	••••
Secret Question	What is my hobby?
Secret Q. Answer	analyzing

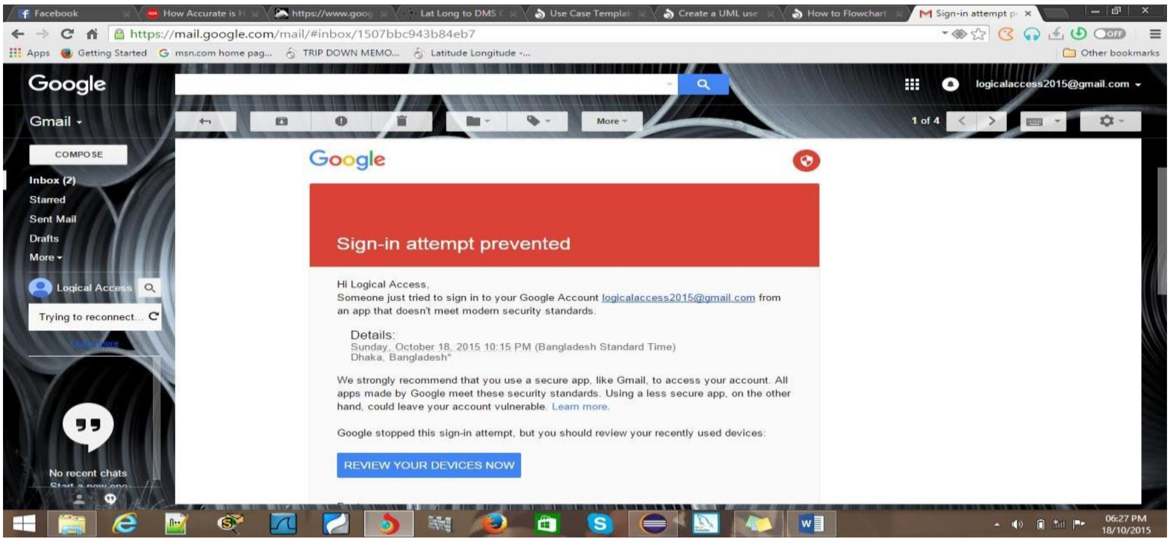
Sign up

03:17 PM 17/10/2015

Fig.3. Showing Registration Page

Figure 3 shows a user registering to the system. The information provided here are stored on the server in the system's backend. The user/employee is requested to supply such information as: Name, Sex, Contact, Username, Password and Secret Question (as a means of alternative login). While the user (Prince_Sule above) enters these details, the web browser prompts a him to share his location, if he clicks on 'Share Location', the application receives and stores the location on the server as a function of geographic coordinates, that is, latitude – longitude. If however the user Prince_Sule declines to share his location, he cannot complete the registration process. If the registration process is complete, the user receives a "Congratulations! You have been successfully registered" message, indicating that he can then proceed to login to the database.

Once Prince_Sule has fully completed the registration process, he is authorized (after due authentication is done) to access the user database with his authentication credentials (username and password) - if his present location matches with the location stored on the server; that is, the location collected during registration.



Google

Sign-in attempt prevented

Hi Logical Access,
Someone just tried to sign in to your Google Account logicalaccess2015@gmail.com from an app that doesn't meet modern security standards.

Details:
Sunday, October 18, 2015 10:15 PM (Bangladesh Standard Time)
Dhaka, Bangladesh*

We strongly recommend that you use a secure app, like Gmail, to access your account. All apps made by Google meet these security standards. Using a less secure app, on the other hand, could leave your account vulnerable. Learn more.

Google stopped this sign-in attempt, but you should review your recently used devices:

REVIEW YOUR DEVICES NOW

Fig.4. Notification of Attempted Unauthorized Access from Bangladesh

Figure 4 shows a notification message sent to the database administrator logicalaccess2015@gmail.com of an attempt at login to the database from a different time zone/country. The system sees this as abnormal and prompts the Google app engine to send a message to that effect to the specified authority.

IV. Discussion of Result

This project solves the burgeoning issue of password theft or compromise and unauthorised access into a password-protected database or environment by ensuring that the location of the user is taken upon registration and enforced for all other subsequent usage of the system. The time feature holds order as location. For the test above, the work limit on the server was set at 08:00 – 17:00 (5 PM). Prince_Sule, although in the verified location was unable to access the database at The location is stored in terms of geographical coordinates, X 0^0 Y^0, that is, Latitude and Longitude. A location of North 9^0 East 6^0 represents the entire region of Minna, Niger State, thus, anyone within this coordinate can access the database with the right authentication credentials (that is username and password) and at working hours.

Changes could be made to the empmodule on the server to increase the system's sensitivity in receiving coordinates For higher precision, the empmodule was set to receive coordinates in Degree Minutes Seconds (DMS), which could be as precise as a pen's ball point. For lower precision, it is set at Degree Decimal, this coordinate could be very precise too but allows a wider roaming capability, thus it could specify an office, a building or a given land mass.

The location N9.5835546 E6.5463156 is a DMS coordinate and represents a computer desk in the east wing of the Cisco lab of the Information Technology Centre (ITS) at the Federal University of Technology Minna, Niger State- location could be that precise. The essence of the location feature of this framework is to ensure that, although a user's password is successfully cracked or stolen, an attacker must be at the exact location where the user/employee registered before he can access the user's system's data or resources; this protects against several forms of attacks, e.g., Sniffing and Brute-force attack.

Spear phishing attacks that target employees and make them give out their login credentials have been one of the most successful form of unauthorized access Hacking situations like the Sony hack of 2014 which occurred as a result of a spear phishing attack can be avoided if location based access controls like this were implemented in the system.

V. Conclusion

Preventing unauthorized access is tantamount to any organization. in this study we presented a system that will check for a devices physical location and match it against an already permissible location, if the location doesn't match then access is denied, it guarantees accessibility to an organizations server and ensures security against identity theft where a genuine users credentials are stolen and used by a malicious user by just logging into the server. it also utilizes time of login to limit an insider attack The architecture of the system presented inherently supports security of enterprise servers, by separating utilizing physical geolocations and time of login as criteria for access to a server. However, this assertion was not evaluated. Hence, this area is open for further studies.

REFERENCES

[1] C Bertolissi and M Fern ández, "Time and location based services with access control," *New Technologies, Mobility and Security, IEEE*, pp. 1-6, November 2008.

[2] T Chothia, D Duggan, and J Vitek, "Type-based distributed access control.," in *Type-based distributed access conComputer Security Foundations Workshop, Proceedings. 16th IEEE*, June 2003, pp. 170

[3] C Ngo, Y Demchencko, and C de Laat, "Multi-tenant attribute-based access control for cloud infrastructure services," *Journal of Information Security and Applications*, 2015.

[4] I Ray and M Kumar, "Towards a location-based mandatory access control model. ," *Computers & Security*, vol. 25, no. 1, pp. 36-44, 2006.

[5] A V Cleeff, W Pieters, and R Wieringa, "Benefits of location-based access control: A literature study.," in *Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing* , 2010, pp. 739-746.

[6] K P Puttaswamy and B Y Zhao, "Preserving privacy in location-based mobile social applications," in *In Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications,ACM* , 2010, pp. 1-6.

[7] J Y Tsai, P G Kelley, L F Cranor, and N Sadeh, "Location-sharing technologies: Privacy risks and controls," *ISJLP, 6, 119*, 2010.

[8] K Curran and J Orr, "Integrating geolocation into electronic finance applications for additional security," *International Journal of Electronic Finance*, vol. 5, no. 3, pp. 272-285, 2011.

[9] A Gross, "Using geolocation in authentication and fraud detection for web-based systems.," Unpublished Master Thesis, Athabasca University. 2011.

[10] S D Ghogare, S P Jadhav, A R Chadha, and H C Patil, "Location based authentication: A new approach towards providing security.," *International Journal of Scientific and Research Publications*, vol. 2, no. 4, pp. 1-5, 2012.

[11] NIST. (2017, June) Digital Identity Guidelines: Authentication and Lifecycle Management. [Online]. https://pages.nist.gov/800-63-3/sp800-63b

[12] E Huseynov and J M Seigneur, "WiFiOTP: Pervasive two-factor authentication using Wi-Fi SSID broadcasts.," in *ITU Kaleidoscope: Trust in the Information Society (K-2015).*, December 2015, pp. 1-8.

[13] J Brassil, P K Manadhata, and R Netravali, "Traffic signature-based mobile device location authentication," *IEEE Transactions on Mobile Computing*, , vol. 13, no. 9, pp. 2156-2169, 2014.

[14] K Curran and J Orr, "Integrating geolocation into electronic finance applications for additional security," *International Journal of Electronic Finance*, vol. 5, no. 3, pp. 272-285, 2011.

[15] CISCO. (2008) Wi-Fi Location-Based Services 4.1 Design Guide. [Online]. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/WiFiLBS-DG/wifich2.pdf

[16] Google. (2017, June) Google Maps APIs. [Online]. https://developers.google.com/maps/documentation/geolocation/intro

[17] Y Shavitt and N Zilberman, "A Geolocation Databases Study," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 10, pp. 2044 - 2056, 2011.

[18] K Harries, "Mapping crime: Principle and practice," *National Institute of Justice*, 1999.

[19] Andre van Cleeff, Wolter Pieters, and Roel Wieringa, "Benefits of Location-Based Access Control: A Literature Study.," in Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom), 2010.

[20] Ghogare D. Shraddha, Jadhav, P. Swati, Chadha R. Ankita , and Patil C. Hima , "Location Based Authentication: A New Approach towards Providing Security," International Journal of Scientific and Research Publications, vol. 2, no. 4, pp. 1-5, April 2012.

[21] Indrakshi Ray and Mahendra Kumar, "Towards a location-based mandatory access control model," Computers and Security, vol. 25, no. 1, pp. 36-44, 2006.

[22] Roselin Chirchi Vanaja and Laxman. M Waghmare, "Iris Biometric Authentication used for Security Systems," Iinternational Journal of Image, Graphics and Signal Processing, pp. 54-60, August 2014.

[23] Olayemi M. Olaniyi, Folorunso A. Taliha , Aliyu Ahmed, and Olugbenga Joseph, "Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking Approach," International Journal of Information Engineering and Electronic Business(IJIEEB), pp. 9-17, September 2016.

[24] Alan Dennis, Barbara Wixom Haley, and M Roth Roberta., *Systems Analysis and Design*, Fourth Edition ed. United States of America: John Wiley & Sons, Inc, 2010.

Authors' Profiles

Victor Legbo Yisa is currently a lecturer in the Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria. He holds a B.Eng degree in Electrical and computer Engineering and an Msc degree in management Information System. Before joining the institution, he served as IT support personnel in an IT firm. His current research interests include cybersecurity, penetration testing Access control, and internet security.

Baba Meshach is currently a lecturer in the Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria. He holds a B.Eng degree in Electrical and computer Engineering and an Msc degree in management Information System. Before joining the institution, he served as IT support personnel in an IT firm. His current research interests include Big data Analytics for security, Access control, and network security.

Oluwafemi Osho is currently a lecturer in the Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria. He holds a B.Tech. degree in Mathematics/Computer Science and an M.Tech. degree in Mathematics. Before joining the institution, he served as Head of the IT Department of one of the leading mortgage banks in Nigeria. His current research interests include cybersecurity, mobile security, and security analysis. He is a Certified Ethical Hacker (CEH).

Anthony Sule is a graduate of Cyber security science from the federal University of technology, Minna. He is the CEO of the online site MIA republic; he has great interest in access control systems. His hobbies are writing and reading.

How to cite this paper: Victor L. Yisa, Baba Meshach, Oluwafemi Osho, Anthony Sule,"Application of Geo-Location-Based Access Control in an Enterprise Environment", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.1, pp.36-43, 2018.DOI: 10.5815/ijcnis.2018.01.05