

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/359659745>

# Anticipation of Cybercrime Threats Pose by eNaira to Nigeria's Economy

Experiment Findings · April 2022

DOI: 10.13140/RG.2.2.34825.52322

---

CITATIONS

0

READS

71

2 authors, including:



[Alhassan Abdulmutallib](#)

Baze University Abuja

4 PUBLICATIONS 0 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Implementation of eGovernment: Reduction of Poverty and Insecurity in Nigeria [View project](#)



Anticipation of Cyber Crime Threats Post by eNaira tom Nigerian Economy [View project](#)

# **Anticipation of Cybercrime Threats Pose by eNaira to Nigeria's Economy**

***Alhassan Abdulmutallib***

*Department of Information Technology Services,  
Baze University, Abuja – Nigeria  
alhassan.abdulmutallib@bazeuniversity.edu.ng*

***Suleiman Sani Bashar***

*School of Architecture & Computer Engineering,  
University of East London  
U1945432@uel.ac.uk*

## **Abstract**

*This study aims to examine the implementation of eNaira by the Central Bank of Nigeria (CBN) as an optimal option to cryptocurrency which the country considered forbidden with an uttermost consideration, also the paper explores the vulnerabilities that are posed by the eNaira implementation to Nigeria's economy, furthermore, the paper provides with recommendations to mitigate the anticipated cybercrime threats.*

**Keywords:** CBN, Cryptocurrency, Cybercrime, Cybersecurity, API.

## **Introduction**

The digital payments scorecard of Nigeria as of 2020 reads 2.7 billion transactions valued at N1.62.9 trillion, which is 1.06 times larger than the size of the country's N154.3 trillion 2020 GDP (eNaira Design Paper, 2021). The Central Bank of Nigeria (CBN) directed all banks to desist from making any transaction that relates to cryptocurrency, also, the CBN directed all banks to terminate any account involved in making cryptocurrency transactions within their banking system (Cryptocurrency Trading: CBN Orders Banks to Close Operating Accounts, 2021). Furthermore, the Central Bank of Nigeria publish a regulatory directive on cryptocurrencies on 7 February 2021 drawing the attention of the Nigerians on dealing with cryptocurrency and also stating their viewpoint on the usage of cryptocurrency, thus, the regulation provides with analogies of countries that prohibit the use of cryptocurrency, thereafter, the CB stated lost incur in transacting with the virtual currency (Response to Regulatory Directive on Cryptocurrencies, 2021).

Nigeria as a country has enormous physical security issues that are fought every day by the state, also it is alarming that, the country Financial Institution has not started to properly consider cybersecurity as a major challenge that might hunt their operations in the future, most of the banking institutions have more than one mobile and web applications for their customers to access their financial savings, it is worthy knowing that, most of the applications that are developed are not conforming to the best practice of software development security approach, a survey has shown, 68 percent of software developers and software development companies are not considering security pipeline during the first phase of the software development process, which is requirement gathering, (Vaughan-Nichols, 2021).

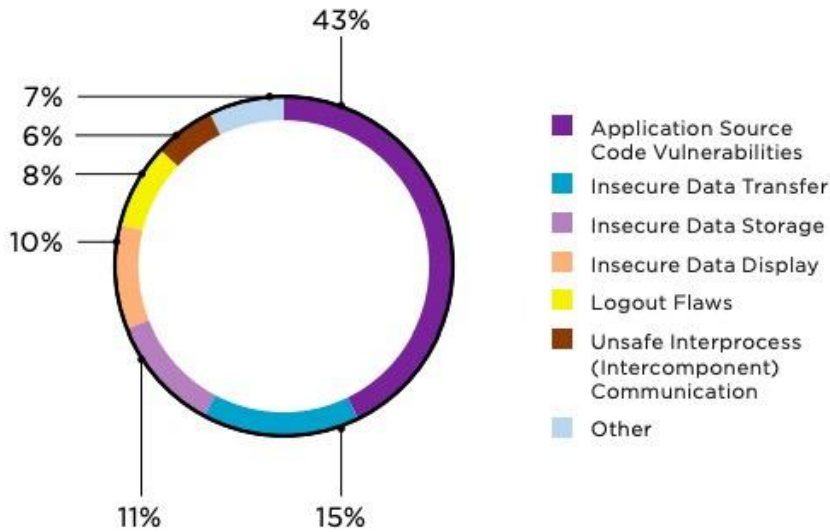
### **Reports of Most Advancing Countries Financial Mobile App that is Vulnerable**

A report of over 150 mobile applications for big companies in the United State of America reveals a high level of security vulnerabilities both on iOS and Android devices, the report shows 77% of those companies have at least one serious vulnerability that could pose a data breach of their client (Intertrust 2021 Report Mobile, 2021).

In the year 2019, Positive Technologies chose 14 fully featured mobile application banking (client and server) for in-depth research to know whether iOS and Android applications for mobile banking are secured, the security level of those chosen applications was assessed manually using the black and gray hacking method with help of automation tools, the summary of the report reveals server-side vulnerabilities in mobile banking application which is related to a faulty application code, the security vulnerabilities where due to failure software updates, lack of proper security implementation from Software Development Life Cycle (SDLC), the

research demonstrated insufficient code protection that is the causes of exploit (Vulnerabilities and threats in mobile banking, 2021)

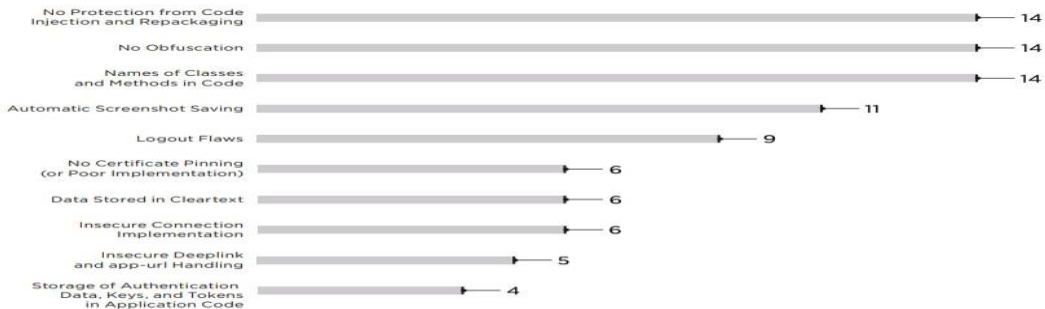
**Vulnerabilities report summary by Positive Technologies**



*Source: Positive Technologies*

Based on the report, attackers can use those vulnerabilities to obtain and access the web server hosting those applications, furthermore, competitors may also want to know how the application is designed to copy new features for their own business goal.

**Vulnerabilities for report summary by Positive Technologies**

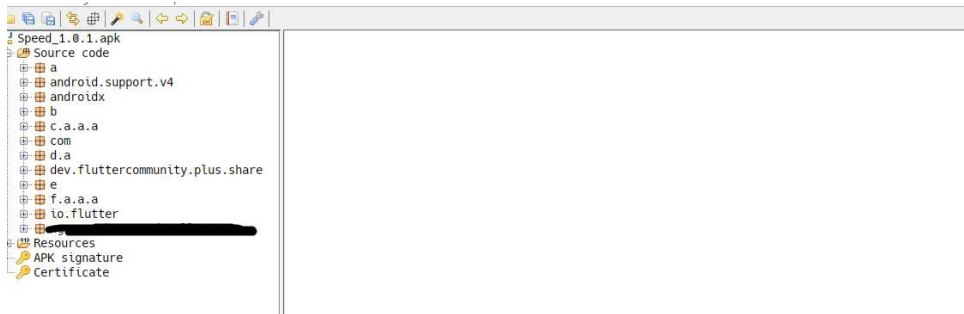


*Source: Positive Technologies*

## Vulnerabilities Found on eNaira Mobile Application

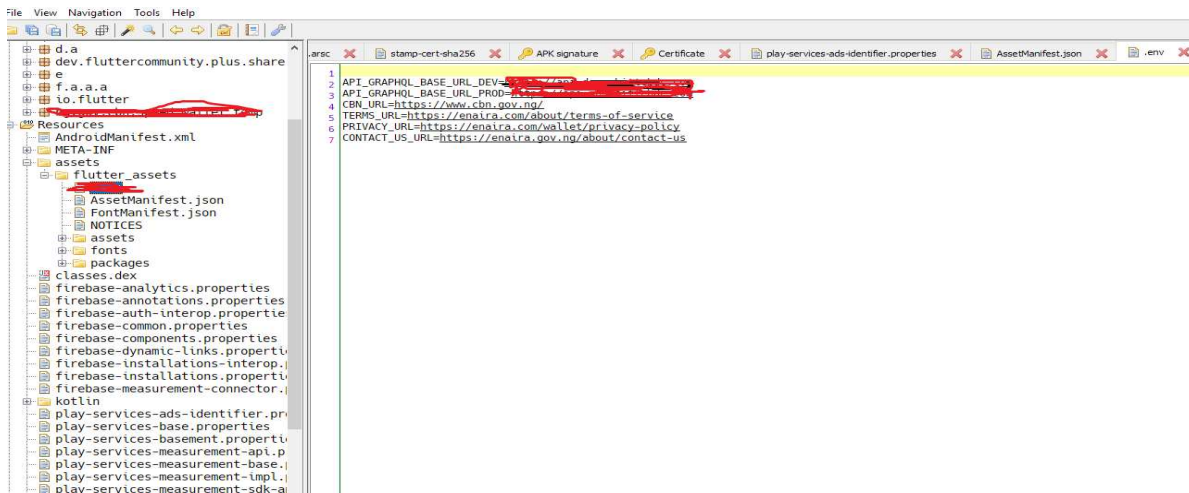
The eNaira mobile application frontend was developed using Java programming language, while the application backend was hosting on a separate hosting environment as shown below;

### Source code of the eNaira application



The code above shows an extracted version of the eNaira mobile application with its structural behavior, this indicates a lack of security prioritization that might leak the application's most valuable location, which is the API endpoint. The second screen capture showcases the most valuable location of the application location, as mentioned above the location to the application API endpoint.

### The eNaira Application Hosting Path



## Other Bugs Issues Found by Users that downloaded the eNaira Mobile Application

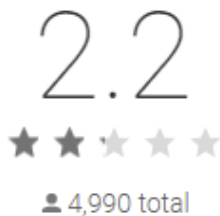
Google Play or Google Play Store was formerly Android Market, is a digital distribution service operated and developed by Google. It serves as an official app store for an Android Operating system application software (Google Play, 2021). The eNaira application was installed by approximately 100,000 users from Google Play, but it is alarming their experience with the system was very poor, based on their rating to the application, a screenshot of the user's experience is shown below;

### Google Play Users Experience with eNaira App

REVIEWS

[Review policy and info](#)

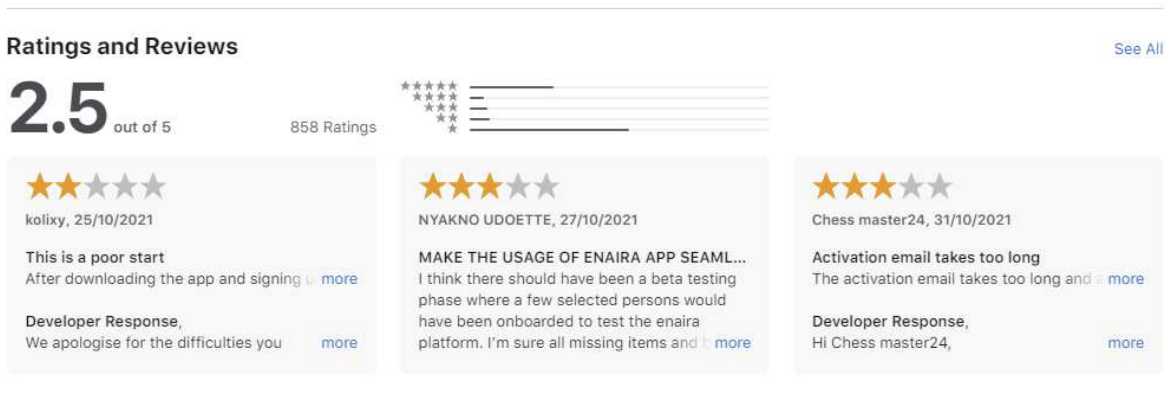
[Write a Review](#)



*Source: Google Play*

App Store is an application store for Apple Inc for their mobile application both iOS and iPadOS. The store allows the users of those devices to download an approved application (App Store (iOS/iPadOS), 2021), as indicated above, most of the Android users has a very poor experience using the application, likewise, the iOS users are experiencing similar problems, below is an aggregational viewpoint of the iOS users;

## *App Store Users Experience with eNaira App*



*Source: App Store*

### **Summary of the Users Experience on App Store and Google Play**

The review from the two application stores indicates that something is missing and there are vulnerabilities on the eNaira application. Our research shows that the eNaira application is on Cloudflare, Cloudflare is a remote proxy for web servers, mostly to protect data from DDoS attacks, but if an application is hosted on a shared hosting environment, cloudflare can fail in serving its purpose, also downtime is a major that could affect the functions of an application, furthermore, the option of securing an application is limited.

### **Recommendations**

According to our findings, the posted vulnerabilities on the application could judgely go to the application developers, as mentioned in the introductory part, the security of applications shall be the major part of the Application Development Life Cycle,



not at the latter, financial companies shall use secured cloud hosting environment like AWS, Azure and many others, that are secured. Also;

- a. Developers shall use obfuscation to make attackers exhausted from analyzing their code.
- b. Passwords shall adhere to Salt hashing.
- c. Code injection and repackaging shall be implemented from the ground root at the application development level.
- d. Developers shall avoid deep linking during application development.
- e. Big companies shall invest in data centres and also, hire professionals to secure their customer's information, not 100 percent relying on third-party protection.

## BIBLIOGRAPHY

Akinkuotu, E., Adepegba, A. and Orjiude, A., 2021. *Vendors fail to embrace eNaira as downloads stall at 220,000*. online Punchng.com. Available at: <https://punchng.com/vendors-fail-to-embrace-enaira-as-downloads-stall-at-220000/> Accessed 1 November 2021.

Enaira.gov.ng. 2021. *eNaira Design Paper*. online Available at: <https://www.enaira.gov.ng/about/design> Accessed 1 November 2021

*Cryptocurrency Trading: CBN Orders Banks To Close Operating Accounts*. 3rd ed. [ebook] Abuja: Ademola Bakare, p.4. Available at: <https://www.cbn.gov.ng/Out/2021/CCD/Volume%203%20Number%202%20CBN%20Update%20February%202021.pdf> Accessed 1 November 2021

*Response to Regulatory Directive on Cryptocurrencies*. [ebook] Abuja: CBN, p.5. Available at: <https://www.cbn.gov.ng/out/2021/ccd/cbn%20press%20release%20crypto%2007022021.pdf> Accessed 1 November 2021

Vaughan-Nichols, S., 2021. *No love lost between security specialists and developers* | ZDNet. [online] ZDNet. Available at: <https://www.zdnet.com/article/no-love-lost-between-security-specialists-and-developers/> Accessed 3 November 2021

Finance.yahoo.com. 2021. *Intertrust Releases 2021 Report Mobile*. [online] Available at: <https://finance.yahoo.com/news/intertrust-releases-2021-report-mobile-160000580.html>, Accessed 9 November 2021

Ptsecurity.com. 2021. *Vulnerabilities and threats in mobile banking*. [online] Available at: <https://www.ptsecurity.com/ww-en/analytics/vulnerabilities-mobile-banks-2020/> Accessed 9 November 2021

En.wikipedia.org. 2021. *Google Play*. [online] Available at: [https://en.wikipedia.org/wiki/Google\\_Play](https://en.wikipedia.org/wiki/Google_Play) [Accessed 11 November 2021

En.wikipedia.org. 2021. *App Store (iOS/iPadOS)*. [online] Available at: [https://en.wikipedia.org/wiki/App\\_Store\\_\(iOS/iPadOS\)](https://en.wikipedia.org/wiki/App_Store_(iOS/iPadOS)) [Accessed 11 November 2021