A Hybrid Identity Based Encryption: A Modest countermeasure for device-to-device (D2D) illegal digital file sharing

Ume Leonard E[1] and Orie Madubuchukwu John[2]

[1,2]Department of Computer Science and Robotics Education
Federal College of Education (Technical), Omoku Rivers State
Email: [1]umeemenike@fcetomoku.edu.ng, [2]madubuchukwu.orie@fcetomoku.edu.ng

ABSTRACT

The innovations in the field of information and communication technology have come with their attendant problems, which require further research to fix. Innovations such as Bluetooth technology, fast wireless internet connections, high memory capacity, etc. have simplified the way in which digital files can be shared among devices. This escalated the problem of copyright piracy, which is a colossal economic sabotage for any nation. To achieve high security and a faster rate of data encryption, a two-pronged security approach was used in this paper, which included the modified EIGamal key exchange algorithm and obfuscation security. To evaluate the performance of this algorithm and techniques, programming was done in HTML5, Java script and PHP to produce a platform for digital file encryption and multi-digital file reader. The testing showed the suggested technique can be used to counter device-to-device sharing of digital files.

.

Keywords: Device-to-device, Copyright piracy, Encryption, file-sharing

African Journal of Computing & ICT Reference Format

Ume Leonard E and OrieMadubuchukwu (2023), A Hybrid Identity Based Encryption: A Modest countermeasure for device-to-device (D2D) illegal digital file sharing

Afr. J. Comp. & ICT, Vol. 16,No. 1/2, pp. 1 –11

1. Introduction

The advancement of information technology has had a reasonable impact on reducing the burden imposed by manual tasks on humanity, particularly in the areas of data processing, storage, and dissemination. For example in the 1980s, the transfer of heavy digital files such as audio files from one computer to another was merely in concept as there were such daunting limitations as to file size, low connectivity bandwidth, the capacity of storage devices, e.t.c[1,2]. These challenges began to fade in the 1990s, thanks to the development of the mp3 file compression standard, which can reduce digital audio files by half their original size, and the introduction of flat rate high bandwidth internet connections [3].This was followed by the development of multi-media computers in the late 1990s, which had more hard disk storage capacity, sound cards, and internal and external speakers.

Another striking innovation is the development of software to rip CDs/DVDs into mp3 files on the computer hard disk and peer-to-peer network applications like Napster, Grokster, Gnutella, Limewire, Kazaa, and eDonkey. These software were not only unrestricted but also took less effort to learn how to use them, which explains its popularity.
This trend of innovation and development has continued to the present, when storage device capacity is measured in terabytes and their sizes have been greatly reduced (micro-memory). Technology has made computers into entertainment devices. The internet has improved so much that developing nations are talking of 5G network deployment whereas work is in advanced stage to deploy 6G in advanced nation. The speed of the internet has made it possible to have paid audio and video file streaming services such as Netflix, iTunes, etc[5, 6].

Furthermore, on the side of interaction among computing devices in terms of data sharing, many innovations have also taken place in that area. The device driver incompatibility errors usually reported by computers when mobile devices are plugged into them have been solved by an upgrade in the operating systems of both computers and mobile devices. The two can easily communicate through the instrumentality of universal serial bus cables, Bluetooth technology, Xender applications, etc. The Xender app can transfer digital files up to 1 GB from one mobile device to the other in less than two minutes [6-8].

Cryptography is a branch of computer security that centers on securing digital information. Encryption is the key branch of cryptography and it simply mean a logical process that scrambles the content of digital information by substitution and rearrangement so that it becomes difficult for an unintended recipient to understand it. Identity based encryption is an aspect of encryption which entails using every user's unique identity such as e-mail address, phone number, etc as the public key. This becomes the user's identifier in the network. The corresponding private key is obtained by some mathematical manipulations which takes the public key and secret master key from trusted authority known as private key generator (pkg) as an input [4].

The motivation for this research stems from a rise in copyright piracy in Nigeria as reported by literatures [11], [16] and the observation of researchers. It is a common sight to see people on the roadside in major towns and cities in Nigeria openly using laptops or PCs to transfer copyrighted digital files such as audio files and video files commercially to their clients for a very paltry sum of money at the expense of the copyright owners (artistes). For example, an audio music album that would cost N500 at regular market price can be transferred to a client illegally at N50 and the buyer can transfer it to his friend at no cost. Due to harsh economic conditions in Nigeria, many Nigerians tend to opt for products or services that are cheaper without considering whether they are legal or not. Meanwhile, the agencies charged with enforcement of copyright laws renege on their responsibilities due to the corruption of some of the officers responsible for that.

Another reason for this study is that, unlike in developed countries where citizens can afford fee-based streaming services like Netflix, the level of poverty and low broadband internet penetration in Nigeria means that such an alternative for paid streaming services cannot thrive in Nigeria for local artists [9],[11]. Some few streaming services, like Airtel Radio, GLO radio can only favour already established artists, but do not favour upcoming artists that are not yet known. According to Owushi [11] and Ume [16], file-sharing eats away opportunities for new artists and a colossal economic sabotage to any nation.

This paper proposes a hybrid security technique that will merge modified EIGamal key exchange algorithm and obfuscation securitytechnique. Firstly, the EIGamal key exchange algorithm was modified to accept the MAC address of the device using the digital file as key in place of large integer number. Secondly, the key (MAC address) is used to encrypt the digital file. Thirdly, the key is as well used to decrypt the digital by authorized user. And finally, obfuscation security technique is used to mask the data (digital file) while in use.

The rest of the paper are organized as follows: section two is the review of related work, material and was in section 3, test and discussion was in section four and section 5 concludes the paper.
.

2. Literature Review

Copyright piracy has long been a problem for humanity, attracting the attention of numerous researchers interested in preventing or at least mitigating its impact, the efforts gained in research to curb or prevent copyright piracy are almost eroded by technological inventions [10]. For instance, the press revolutionised the spread of knowledge in all fields of human endeavour, as well as increasing literacy in the broader community. However, it also introduced an entirely new problem for intellectual property owners; prior to the press, it was such a big task to make copies of books or other printed materials in volumes, which discouraged any illegal duplication for economic gain, but the press technology instantly changed all that as it became easier to make copies faster and at a cheaper rate. This made both the publishers and authors of such works seek protection, both for economic reasons and to ensure that their works remained unaltered and the authors were duly credited [7].

Similarly, the heterogeneous nature of information technology devices gave rise to technologies that facilitated device-to-device (D2D) communication, such as Bluetooth technology,

Wifi, Mp3, Xender app, BitTorrent, etc. This good-intentioned innovation posed a platooning problem of copyright piracy, as copies of digital files (both the ones protected by copyright law) can be shared among devices at the speed of light and without trace [10]. Recent research on tracking D2D data sharing has focused on cryptography-based approaches such as Identity Based Encryption (IBE), Certificateless Public Key Encryption (CPKE), Digital Right Management (DRM), Content Poisoning System (CPS), and Chaotic Block Cipher Encryption (CBCE), which played an important role in bringing a solution to the problem.

Identity Based Encryption (IBE) is the concept that allows an arbitrary string bit like the user's email or phone number to be his identifier, which of course is the public key [6]. The corresponding private key is obtained by some mathematical manipulations which take the public key and secret master key from a trusted authority known as a private key generator (PKG) as an input. The shortcomings of IBE rest on an unconditional trust that must be placed on the PKG, and the PKG can impersonate any single entity as everyone's private key is known to the PKG. Horwiz and Lynn [9] proposed the concept of two level hierarchical identity-based encryption (2-HIBE) to address the apparent shortfall of IBE. The 2-HIBE system consists of two key generators, namely root PKG and domain PKG. Collusion resistance was ensured at the upper level domain by the two 2-PKGs, and partial collusion resistance was ensured at the lower level. This to some extent prevents unauthorised access to some digital data, especially text-based data. However, the IBC cannot adequately help track the identity of a particular user of digital files since one person can have multiple e-mails.

Certificateless Public Key Encryption (CPKE), which was an approach introduced to handle the limitations that resulted from identity based encryption [1]. The basic concept of CPKE was proposed by Al-Riyami and Peterson [1] as a model where the user's public key is no longer an arbitrary string but rather it is similar to the public key used in the traditional PKC generated by the user. The public key generated by this model does not need to be explicitly certified since it has been generated using some private key obtained from some trusted authority known as the Key Generation Centre (KGC). KGC does not know the private keys of users, thereby addressing the limitations of IBC. Some studies [6], [12] also deepened research in this direction, but the limitation still lies in the physical implementation of the model as it is expensive to implement.

A signature scheme, especially a group signature, is a cryptographic scheme used to secure data in device-to-device communication. This scheme offers anonymity and unlinkability for the channel users. According to Xie, *et al*. [17], each group member has a private key and signs a message anonymously on behalf of the group. Other members use a shared group key to validate signed messages without divulging the identity of the person who signed them.
Homomorphic encryption (HE) is another cryptographic scheme used to secure data in d2d communication, essentially useful when requesting data from untrusted entities. It allows users to perform operations on encrypted ciphetext without knowing the original data [2]. Therefore, HE produces the same encrypted result in ciphertext as the operation executed on plaintext. This is very useful in an environment where the computation occurs on servers that do not trust each other. Mu and Bakiras [2] applied this method to privately identify whether friends are within a nearby distance without actually revealing their identity.

The public key infrastructure (PKI) model is a cryptographic scheme in which each participating device in D2D communication has both private and public keys to authenticate messages. Nevertheless, it requires that PKI be adapted to fulfil several privacy requirements. Certificates should not include identifying information about the owner. And the key should be changed periodically to circumvent the linking of signed messages by the same certificates. Raya &Hubaux [13] came up with an approach where each user obtains two certificates. A distinctive long key identity is shared jointly with a key pair and multiple pseudonyms associated with anonymous key pairs to sign messages. In securing data between d2d communications [8], they noted that key management and distribution is a challenge, which prompted them to leverage the single sign on and authorization mechanism as applied in social network applications like Facebook.

3. Materials and Methods

Securing sensitive data is a critical aspect of any information system as illegitimate users work round the clock to pull down any security method in place [15]. It is on this premise that the proposed system adopts hybrid security approach as shown in figure 1 to tackle the protection of digital files in other to mitigate or to stop device-to-device transfer of such data. The hybrid security approach adopted are cryptographic security and obfuscation security. The reason for this twofold security is that previous solutions to the problem of illegal transfer of digital files from device to device had shown that when an authorised user purchases such a file, s/he is entitled to use it (decrypt it). The issue lies in the fact that the file in its decrypted state can be transferred to a third party, which would constitute a breach of copyright laws. The two-pronged approach ensured that the limitation of third-party transfer was handled as cryptography took care of the encryption of the digital file and obfuscation security handled the aspect of masking the digital file in the client's device.

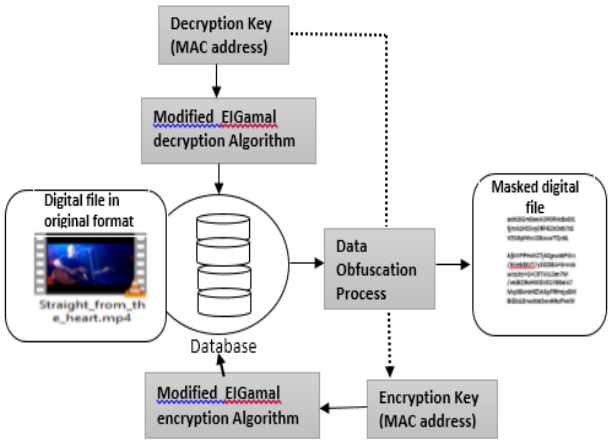


Figure 1: Graphic view of hybrid identity-based encryption

3.1 Cryptographic security:
Cryptography is information science that scrambles information by rearrangement and substitution of the content, making it unfit for anyone to understand except a person equipped to unscramble it. This is achieved by some mathematical computations. The cryptographic security proposed is identity based encryption system based on EIGamal key exchange algorithm [6] and the selective encryption technique algorithm (SETA) for audio and video file [8]. The EIGamal key exchange algorithm was later modified to use MAC address of the using machine as both the encrypting key and the decrypting key. The SETA was employed because the digital file of interest in this research are audio and video files.

EIGamal key exchange algorithm: This algorithm has three phases.

- Key generation phase:
  - *Choose a large prime number g, make a choice of another number h which is a primitive root of g*
  - *Generate a random integer X, such that 1 < X < g-1*
  - *Computer Y = gX mod hSender*
  - *private key is X and the public key is {h, g, Y}*
- Encryption of Message
  - *Represent the message as an integer M in the range of $0 \leq M \leq p - 1$*
  - *Choose a random integer k such that $1 \leq k \leq g - 1$Compute*
  - *a one-time key $K = (Y)^k \bmod h$*
  - *Encrypt M as pair of integers (C_1, C2)*
  - *C1 = h mod p, C_2 = (KM) mod g*
- Decrypting the Message
  - *Recover the key by computing K = (C1)x mod g Compute M = (C2K-1) mod g*
  -

Modified EIGamal Algorithm

- Key generation phase:
  - *Get the Media Access Control (MAC) address of the device represented by Q*
  - *Choose a large prime number g, make a choice of another number h which is a primitive root of g*
  - *Generate a random integer X, such that 1 < X < g-1*
  - *Computer Y = gX mod h*
  - *Sender's private key is Q*
- Encryption of Message
  - *Represent the message as an integer M in the range of $0 \leq M \leq p - 1$*
  - *Choose a random integer k such that $1 \leq k \leq g - 1$Compute*
  - *a one-time key $K = (Y)^k \bmod h$*
  - *Encrypt M as a pair of integers (C_1, C2)*
  - *C1 = h mod p, C_2 = (KM) mod g*
- Decrypting the Message
  - *Recover the key by computing KM = (C1)x mod g Compute M = (C2M-1) mod g*

Selective Encryption Technique Algorithm for Video and Audio Data
This type of algorithm only encrypts the selected bytes in the video frame. It has lower computational capacity to a great degree because every bit is not required to be encrypted. The merit of this algorithm is that it is very fast, but the encryption ratio is low [14]. The reason for using this is that it saves time and has a low computing resource requirement.

Encryption:
The following stages are involved in encryption:

- *Read the original video*
- *Extract 'j' frames from the video as JPEG images.*
- *Convert JPGE images into blocks of 128 bits each.*
- *Encrypt the block with the key, in this case the MAC address, using the EIGamal algorithm.*
- *Convert the encrypted frame to video again.*

Decryption:
The stages in encryption are carried out in reverse order.

3.2 Obfuscation Security:
This is a security procedure where data and other important components of a system, such as software codes, addresses, e.t.c., are masked from a second-party user in order to protect the data from unauthorized access. The focal point in obfuscation is that any data masking should not change the

actual meaning of such data. In this research, we employed address obfuscation, whereby the legal user (second-party) of the copyright file will not know the address where the decrypted file is copied to while in use. This ensured that the copyright file continued to be in its encrypted state.

4. Test and Discussion

To evaluate the performance of this algorithm (modified EIGamal key exchange algorithm and the selective encryption technique algorithm for audio and video files) and obfuscation technique, were implemented in programming using HTML5, PHP and Java script which produced a platform for digital file encryption and multi-digital file reader. The multi-digital file reader is integrated in the sense that it can view digital images, play audio, play video, and view e-books. The function to decrypt any file encrypted using the MAC address as the encrypting key was embedded in the player. It requires the same key to decrypt.

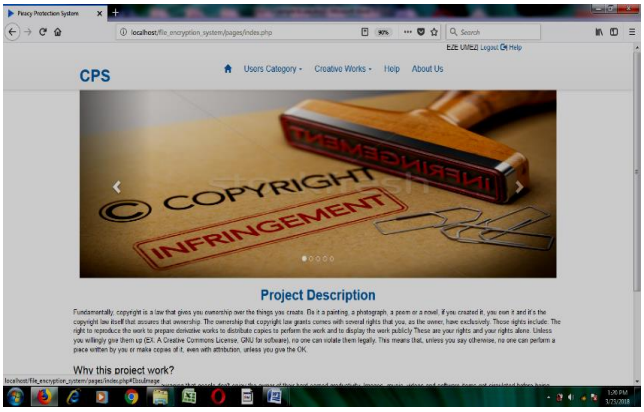


Figure 2: Main interface

This is the interface where copyrighted digital content owners will upload their digital files (audio, video, images, and e-book) for the purpose of protection (encryption). The digital files tested includes digital image, video music digital file, eBook file, and audio files. The entire file was encrypted. The platform also provides access to other categories of users who wish to use this content either for free or at a paid price depending on the owner of the work. To download any of the files, the system will require registration of the device to which the file(s) will be downloaded in order to track usage, particularly by unauthorised third-party users. One of the essential data to capture during the registration is the device's unique identity, which in the case of a computer system is the MAC address, and a mobile device is the IMEI number.

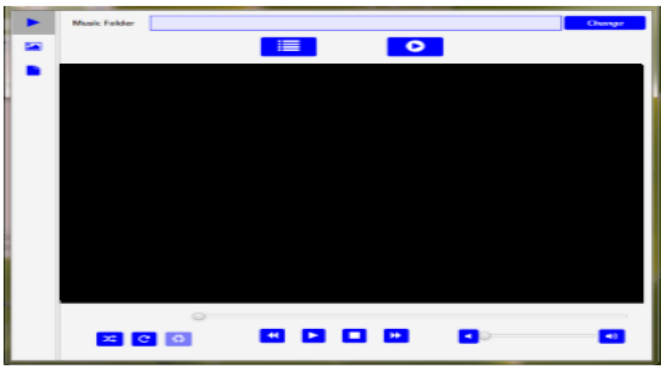


Figure 3: Multi-digital file reader interface

The multi-digital file reader shown in Figure 2 is the other leg of the project. This interface is used to read the digital files downloaded from the platform in Figure 1, which are in encrypted form. The reader is capable of reading digital audio, digital video, digital images, and e-book. The user selects the file type to be read and will be prompted by the reader to enter the device identity number as shown in Figure 3. The device's identity number serves as the decrypting key. The file reader also has the capability to delete the decrypted file after usage immediately to avoid third party transfer.

Figure 4: Multi-digital file reader authentication interface

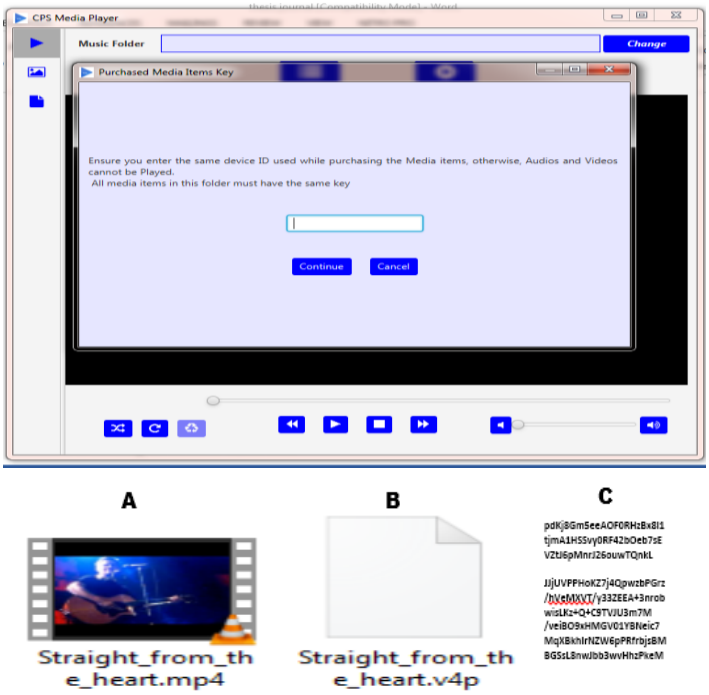


Figure 5: Sample of a digital file at different stages

Figure 4 shows various formats of the digital file. The digital file tested in this case was foreign music video file. The entire file was tested. The image labelled "A" is the file in its original format, the one labelled "B" is the file after the encryption at the front end of the application, whereas the image labelled "C" is the file after encryption at the backend. The file downloaded by the user is in the format represented by the one labelled "B." The essence is to show the format of digital file when it is on its own and when the software is applied to it.

5. Conclusion

In this research, a technique for data encryption has been presented. This employs the device identity numbers of receiving devices as the encryption and decryption keys which for personal computers are the MAC address and for mobile devices, the IMEI number. The entire process, used two algorithms for its implementation. First, is the modified EIGamal key exchange algorithm and secondly is the obfuscation security algorithm. The multi-digital file reader which is designed to read the encrypted files has an inbuilt obfuscation security that ensures that the decrypted file is hidden from the user and deleted immediately after reading. The project made a good attempt to curb rampant authorized transfer of digital files from device-to-device. This will invariably reduce the incidence of copyright theft which is reaping off on the economy of any nation. Copyright theft is simply economic sabotage to the economy of any nation

References

[1] Al-Riyami, S. S., & Paterson, K. G. (2003, November). Certificateless public key cryptography. In *International conference on the theory and application of cryptology and information security* (pp. 452-473). Springer, Berlin, Heidelberg.

[2] Mu, B., &Bakiras, S. (2016). Private proximity detection for convex polygons. In *Proceedings of the 12th International ACM Workshop on Data Engineering for Wireless and Mobile Access* (pp. 36-43).

[3] Baek, J., Safavi-Naini, R., & Susilo, W. (2005, September). Certificateless public key encryption without pairing. In *International conference on information security* (pp. 134-148). Springer, Berlin, Heidelberg.

[4] Batamuliza, J &Hanyurwimfura,D.(2021) Identity based encryption with equality test , Information Security Journal: A Global Perspective, 30:2, 111-124 DOI: 10.1080/19393555.2020.1811924

[5] Canetti, R., Halevi, S., & Katz, J. (2004, May). Chosen-ciphertext security from identity-based encryption. In *International conference on the theory and applications of cryptographic techniques* (pp. 207-222). Springer, Berlin, Heidelberg.

[6] Cheng, Z. (2007). *Pairing-based cryptosystems and key agreement protocols* (Doctoral dissertation, Middlesex University).

[7]Ghazi, K. (2012). Game piracy examined. Retrieved from http://www.tweakguides.com/piracy_4.html

[8] Haus, M., Waqas, M., Ding, A. Y., Li, Y., Tarkoma, S., & Ott, J. (2017). Security and privacy in device-to-device (D2D) communication: A review. *IEEE Communications Surveys & Tutorials*, *19*(2), 1054-1079.

[9] Horwitz, J., & Lynn, B. (2002, April). Toward hierarchical identity-based encryption. In *International conference on the theory and applications of cryptographic techniques* (pp. 466-481). Springer, Berlin, Heidelberg

[10] Mansell, R., &Steinmueller, W. E. (2013). Copyright infringement online: The case of the DigitalEconomy Act judicial review in the United Kingdom. *New media & society*, *15*(8), 1312-1328.

[11] Owushi, E. (2020). Protecting Copyright Owners in Nigeria: A Panacea for Intellectual Development. *International Journal of Knowledge Content Development & Technology*, *10*(1), 21-34.

[12] Qu, H., Yan, Z., Lin, X. J., Zhang, Q., & Sun, L. (2018). Certificateless public key encryption with equality test. *Information Sciences*, *462*, 76-92.

[13]Raya, M., &Hubaux, J. P. (2005, September). The security of VANETs. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks* (pp. 93-94).

[14]Sharma, S., &Pateriya, P. K. (2012). A study on different approaches of selective encryption technique. *International Journal of Computer Science & Communication Networks*, *2*(6), 658.

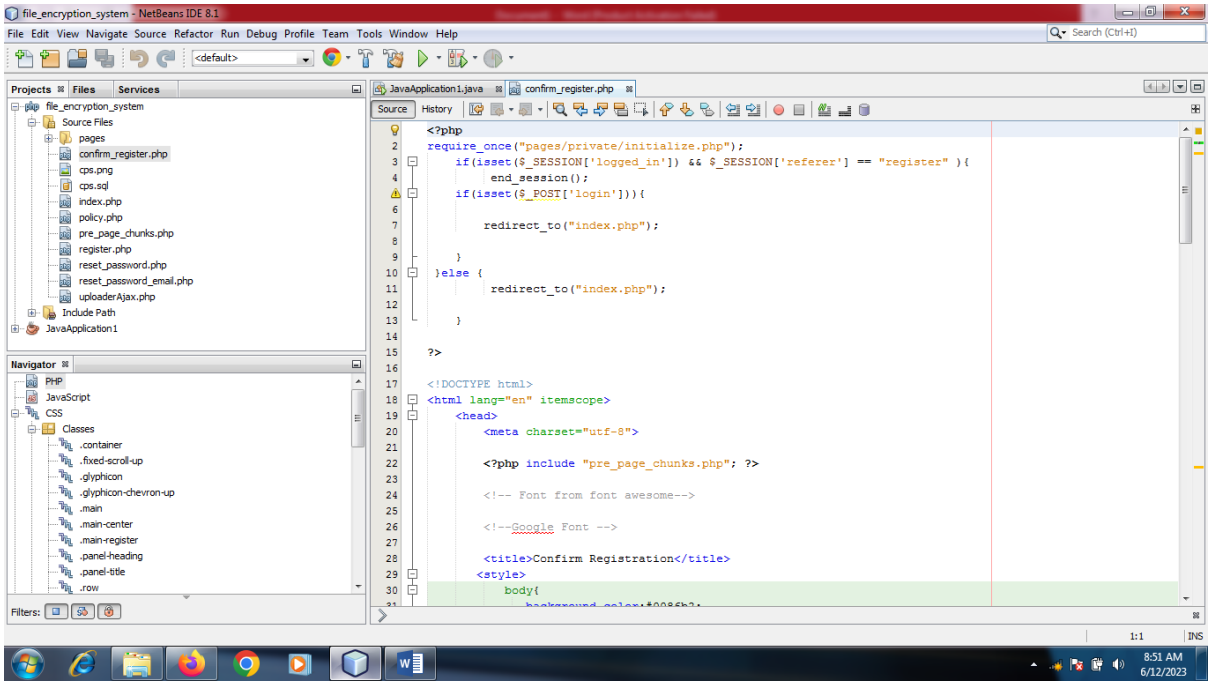
[15] Thirumalaisamy, M., Basheer, S., Selvarajan, S., Althubiti, S. A., Alenezi, F., Srivastava, G., & Lin, J. C. W. (2022). Interaction of secure cloud network and crowd computing for smart city data obfuscation. *Sensors*, *22*(19), 7169.

[16] Ume, L. E. (2021). Technological countermeasures of copyright piracy enforcement in Nigeria: An alternative to creative works owners' livelihood in a monolithic economy post covid-19. *Library Philosophy and Practice*, 1-9.

[17] Xie, Y., Ding, W., & Wang, Y. (2016). A More Extensible Transparent Encrypted File System Based on Filter Driver. *J. Commun.*, *11*(4), 383-387.

Appendix B

Source Programs




```
<?php
require_once("pages/private/initialize.php");
if(isset($_SESSION['logged_in'])){
   end_session();
}
if(isset($_POST['btn-login'])){
   //start session now
   if(!isset($_SESSION)){
      session_start();
   }
   $pass = md5(sql_prep($_POST['password']));
   $email = strtolower(sql_prep($_POST['email']));
   $category = $_POST['category'];
   $error = array();


   if(!empty($email) && filter_var($email, FILTER_VALIDATE_EMAIL) && $category != "none"){

      $sql=mysqli_query($mysqli,"SELECT * FROM users_tb WHERE email='$email' AND password='$pass' ");


         //This is for the login process

            $cout=mysqli_num_rows($sql);

            if($cout>0){
               $row=mysqli_fetch_array($sql);
```

```
            $_SESSION['id'] =strtolower(trim($row['user_id']));
            $_SESSION['category'] =strtolower($category);
            $_SESSION['hint'] =strtolower(trim($row['pass_hint']));
            $_SESSION['first_name'] =strtolower(trim($row['f_name']));
            $_SESSION['last_name'] =strtolower(trim($row['l_name']));
            $_SESSION['answer'] =strtolower(trim($row['answer']));
            $_SESSION['email'] =strtolower(trim($row['email']));
            $_SESSION['phone'] =strtolower(trim($row['phone']));
            $_SESSION['address'] =strtolower(trim($row['address']));
            $cat_from_db = strtolower(trim($row['user_category']));

            if($cat_from_db =="admin" || $cat_from_db == "artist"){

                $sql=mysqli_query($mysqli,"SELECT brand_name FROM artist_tb WHERE email='{$email}' ");
                 $count=mysqli_num_rows($sql);
                 if($count > 0){
                    $row = mysqli_fetch_array($sql);
                     $_SESSION['brand_name'] = $row['brand_name'];
                 }

            }
            if($cat_from_db == "admin"){
                $_SESSION['category'] = $cat_from_db;
            }



                enterLoginDetail($mysqli, $row['category'] , $email);
                //update last login
                $last_login = time();
                mysqli_query($mysqli, "UPDATE users_tb SET last_login = {$last_login} WHERE email = '{$email}'");
                after_successful_login();
          redirect_to("pages/index.php");
} else {
            $error['incorrect_data'] = "Email or password do not match.";
            enter_report_db($mysqli,$email, "An attempt to login");
        }
      } else {
    $error['email_error'] = "incorrect email or email empty";
  }

}
 function enterLoginDetail($mysqli, $category , $email){
    $login_error = array();
  $ip = $_SERVER['REMOTE_ADDR'];
   $browser = $_SERVER['HTTP_USER_AGENT'];
      if(trim($ip) ==""){
    $ip = "none";
  }
  if(trim($browser) ==""){
     $browser = "none";
  }
    date_default_timezone_set("Africa/Lagos");
  last_login = date("Y-m-d H:i:s");
    $session_id = session_id();
    //add the details to the database, include email
   $sql = "INSERT INTO login_details_tb (email, session_id, ip,  browser, category, date)
    VALUES (?,?,?,?,?,?)";
    //Prepare the statement
    $stmt = $mysqli->prepare($sql);
   //Checking prepared error
```

```
    if(!$stmt) {
        //die("Prepare failed: (" . $mysqli->errno . ") " . $mysqli->error);
        $login_error['prepared_statement'] = "error in prepared statement";
      }
      //Binding the resutl
      $bind_result = $stmt->bind_param("ssssss", $email, $session_id, $ip, $browser, $category, $last_login);
      //Binding error
      if(!$bind_result) {
        //echo "Binding failed: (" . $stmt->errno . ") " . $stmt->error;
         $login_error['binding_error'] = "Binding error";
      }
      // 4. Execute
      $stmt->execute();
      //Execution error
      if($stmt->errno) {
       //echo "Execute failed: (" . $stmt->errno . ") " . $stmt->error;
         $login_error['execution_error'] = "Binding failed: (" . $stmt->errno . ") " . $stmt->error;
      }
      // 8. Close statment
      $stmt->close();
      // 9. Close MySQL connection
    // $mysqli->close();
        if(!empty($login_error)){
        $login_error['error'] = "error";
        return $login_error;
      } else{
        return ["success" => "success"];
      }
}
?>
<!DOCTYPE html>
<html lang="en" itemscope>
<head>
<meta charset="utf-8">

<?php include "pre_page_chunks.php"; ?>

<!-- Font from font awesome-->

<!--Google Font -->

<title>Login - Piracy Protection System</title>
<style>
        body{
          background-color:#f2f2f2;
        }
</style>
</head>
<body id="login-page">
<div class="container">
<div class="row main">
<div class="panel-heading">
<div class="panel-title text-center">
<h1 class="logo-text"> CPS </h1>
<hr>
<h3 class="logo-text">Login</h3>
</div>
</div>
<div class="main-register main-center">
<form class="form-horizontal" method="post" id="login-form" >
```

```
<div id="error" class="text-danger"><span class="glyphicon glyphicon-alert"></span><span id="errorMessage">Error Loggin in.</span></div>

<br>
<div class="form-group">

<div class="col-lg-12">
<label for="firstName" class=" control-label">Email</label>
<div class="input-group">
<span class="input-group-addon"><i class="glyphicon glyphicon-user" aria-hidden="true"></i>
<input type="email" required name="email" id="email" placeholder="Enter Your Email" />

</span>
</div>
</div>
</div>

<div class="form-group">

<div class="col-sm-12">
<label for="password" class=" control-label">Password</label>
<div class="input-group">
<span class="input-group-addon"><i class="fa fa-key" aria-hidden="true"></i>
<input type="password" required  name="password" id="password" placeholder="Enter Your Password" />
<!--<span class="togglePassword">show</span>  -->
</span>
</div>
</div>
</div>
<div class="form-group">
<div class="col-sm-12">
<label for="category" class=" control-label">User Category</label>
<div class="input-group">
<select required id="category" class="form-control" name="category" style="border:0px; margin-left:10px;">
<option value="none">--select--</option>
<option value="artist">Copyright Owner</option>
<option value="customer">Customer</option>

</select>

</div>
</div>
</div>
<div>
<?php
            if(!empty($error)){
               echo '<pre>';

               foreach ($error as $key => $value){
                  echo $value ."<br>";
               }
               echo '</pre>';
            }

         ?>

</div>
<input type="hidden" name="btn-login" value="btn-login">
<div class="form-group" style="width:100%">
<button type="submit"  name="btn-login" value="button" class="btn btn-primary btn-md login-button pull-left" id="login-button">
```

```
                    Login <span class="glyphicon glyphicon-log-in" id="login-icon"></span><span class="fa fa-spinner fa-spin" id="spinner"></span>
</button>
<button type="reset"  class="btn btn-primary btn-md  login-button pull-right" id="reset-button">
                    Reset
<span class="glyphicon glyphicon-trash" aria-hidden="true"></span>
</button>

</div>
<div class="login-resister" style="width:100%;">
<span class="text-left" style="width:50%;"><a href="register.php">New User</a></span>
<span class="pull-right" ><a href="reset_password.php" >Forgot Passord?</a></span>
</div>
</form>
</div>
</div>
</div>
<a href="#login-page" id="scroll-button" class="fixed-scroll-up">
<span class="glyphicon glyphicon-chevron-up"></span>
</a><!--scroll-button-->

<script type="text/javascript">
    $(document).ready(function(){
        //Hide the spinner
        $("#spinner").hide();
        //Hide the error div
        $("#error").hide();
            $("#login-button").on('click', function(e){
            e.preventDefault();
             var email = $("#email").val().trim();
            var password = $("#password").val().trim();
            var category = $("select#category").val();
                 if(email.length == 0 || password.length == 0 || category =="none"){
                $("#errorMessage").html("Wrong Email or Password");
                $("#error").show();
               return;
            } else{
                $("#error").hide();
            }

            //var button = $(e.target);
           //var data = button.parents("form").serialize() + '&' +
              //encodeURI(button.attr('name')) + '=' + encodeURI(button.attr('value'));
            //var data = $("#login-form").serialize() + '&' + encodeURI('btn-login')  + '=' + encodeURI('btn-login');
            //console.log(data);
```