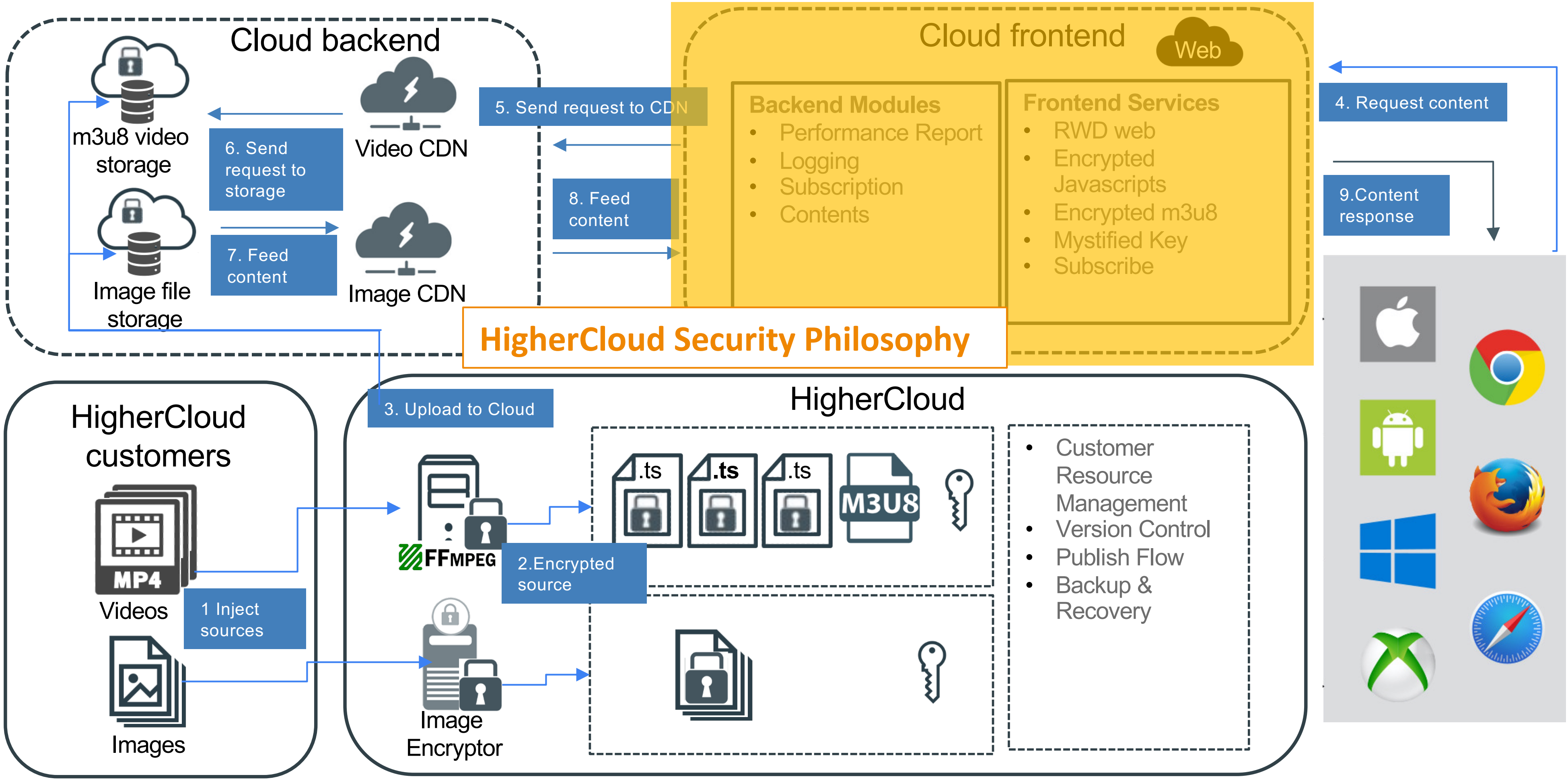
Present by Kevin Chen

2021-07-28

The HigherCloud Solutions HLS Encryption & High Secure VOD Streaming

A security design to effectively prevent video interception

The HigherCloud Solution



Cloud backend

m3u8 video storage

Image file storage

Video CDN

Image CDN

6. Send request to storage

7. Feed content

5. Send request to CDN

8. Feed content

Cloud frontend

Web

Backend Modules
- Performance Report
- Logging
- Subscription
- Contents

Frontend Services
- RWD web
- Encrypted Javascripts
- Encrypted m3u8
- Mystified Key
- Subscribe

4. Request content

9.Content response

HigherCloud Security Philosophy

HigherCloud customers

MP4

Videos

Images

1 Inject sources

HigherCloud

3. Upload to Cloud

FFMPEG

2.Encrypted source

.ts

.ts

.ts

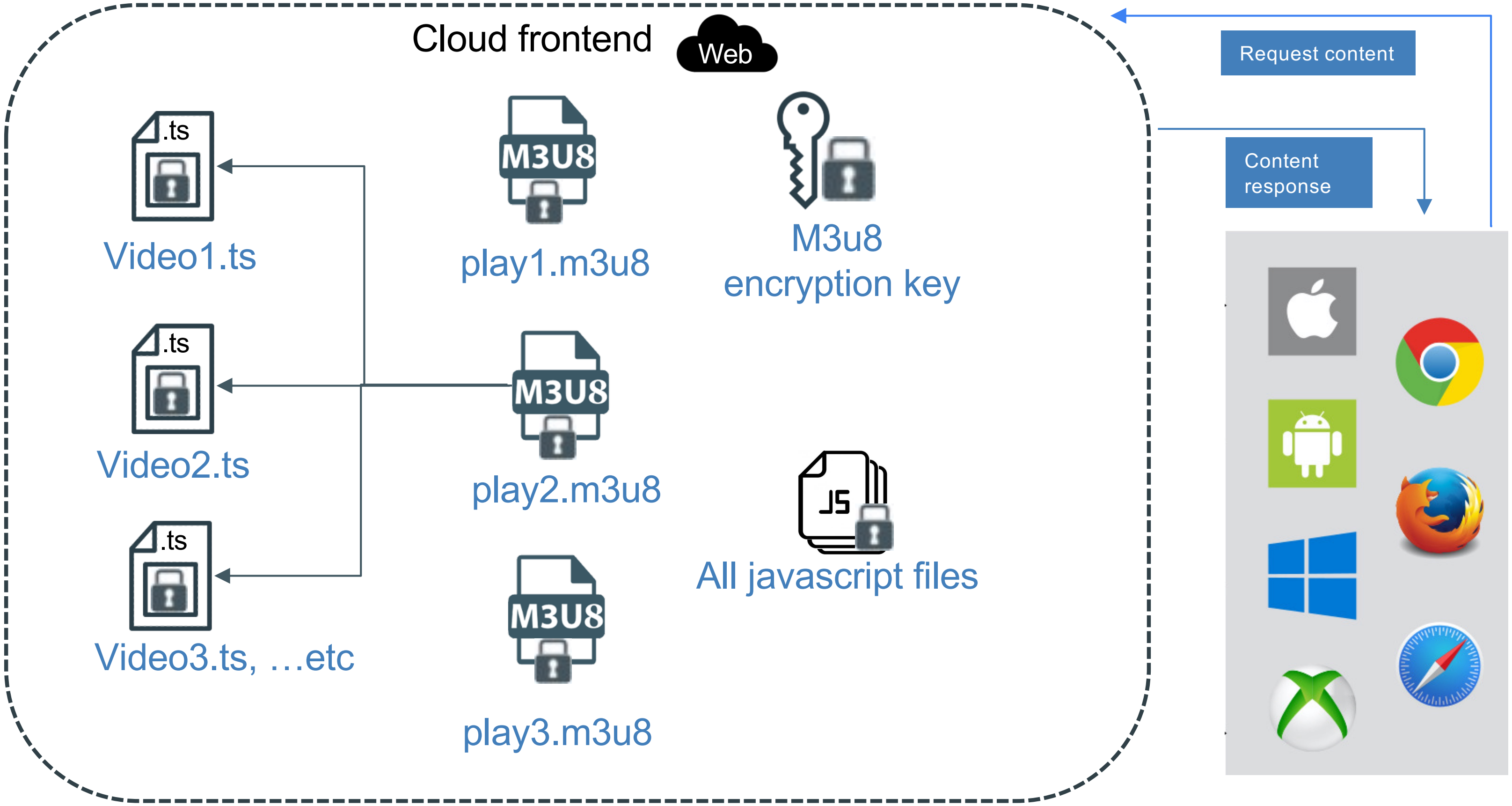
M3U8

Image Encryptor

- Customer Resource Management
- Version Control
- Publish Flow
- Backup & Recovery

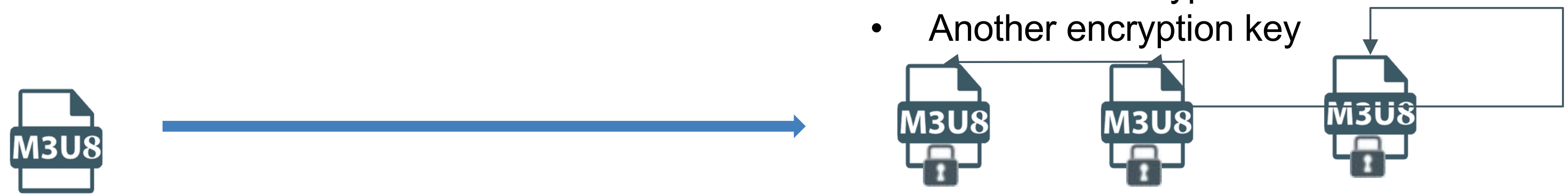
Security Design

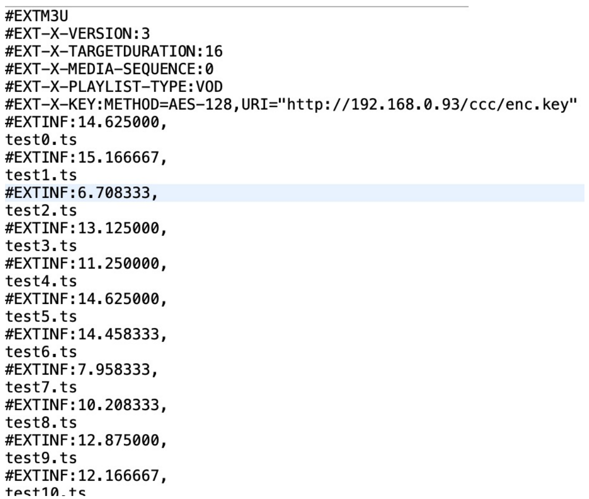
All contents requested from browser is encrypted or mystified



Secured m3u8 & Encryption Key

- 1 real and 2 dummy m3u8 playlists
- Content encrypted with AES-128
- File name encrypted
- Another encryption key





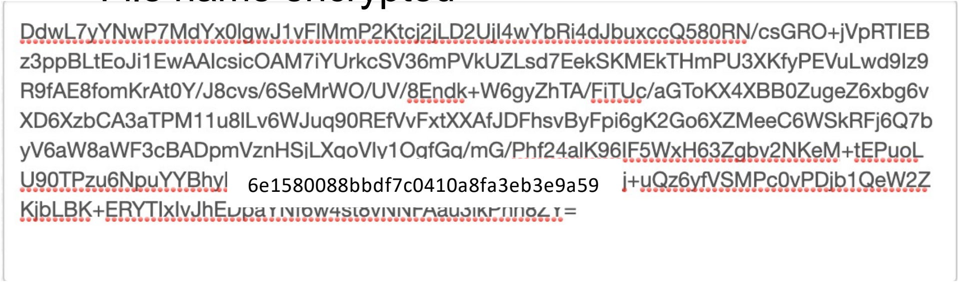
```
#EXTM3U
#EXT-X-VERSION:3
#EXT-X-TARGETDURATION:16
#EXT-X-MEDIA-SEQUENCE:0
#EXT-X-PLAYLIST-TYPE:VOD
#EXT-X-KEY:METHOD=AES-128,URI="http://192.168.0.93/ccc/enc.key"
#EXTINF:14.625000,
test0.ts
#EXTINF:15.166667,
test1.ts
#EXTINF:6.708333,
test2.ts
#EXTINF:13.125000,
test3.ts
#EXTINF:11.250000,
test4.ts
#EXTINF:14.625000,
test5.ts
#EXTINF:14.458333,
test6.ts
#EXTINF:7.958333,
test7.ts
#EXTINF:10.208333,
test8.ts
#EXTINF:12.875000,
test9.ts
#EXTINF:12.166667,
test10.ts
```

1zQXMj65m9UG8LrsvdHWOGWZ8xO0zKqTG9OBz4+RvFnmDsxQRHuu0dAN/
kXPnPLy5EL9yNvL1VzWnmbvoAYZtAUTW7sfQsYyjSBUERoyd8t+NNSafkAYBSv0zuQNw9PlXedMz5cEoQiLt11m9ZETGXASziSo5206Eus0Fe
K1qNHfejljsQalxgz21R7J+S0HlcBOV+lhBWxdbQy7YEBlanKfHlZZJZ8zcJlrx9HHkJhedGpUCEuUq9NwNgVmYwHKvp7UqH7OYyHWUXF6Bce
8XIVhtlNb9MlfGDcr/
Sjcz5Bc+t4RTD7MZbQT8sqNQHtQmh0GgTBlGzi7Dq3vY3ksr2hs2QvYXVSrTjCaN5nCsrFhCvTokOcVdUk7Tl5SlxUrsxjlWj/
vX2xiLcPLut2djRfTxD0TsDgr8g9E1zXCbP98vW8F+DK5nk2ULxEFTvSljOoiQoGjlMGXiXP6nOil4H1yuMHYhPy9pT4/
TLuusfLQmmVIW3tuU+4TMO1AWLUVGFNnpk4E22ORVjel8l7bf6Yb2zyZuUV8ZRylotBbY3ncQZE9vkwllgxYeUGQhE+Pk9bFJwLNsQpjiq3i4A
R9Skhpi269x4JH1gkrlCkldw7wwyFYUs9kJrOro3W7AHzDdzF2GzU+Splv/
6J0kzEYyn1ywSuC9L8pcUQdBTtgPGEipmirNLaEJJVdGKoMJbEZml1OO/
vHSGmKYCd44dwwyQ3aP+YuYdch6OuhzE5nAn0h9ltLjGYZKHECZkh0rDBnNFCSOAT1WHy6Ghbxvy+h1a9zFRCMBQ730C/
qD9V3buyLNuYSwVGLTJ0O5SlTQKuSaRsKglpgGCObhRaGlgpCpEJFojBaTGyrKmf7rMVhaaLR/
GDM6fX4SNYtjC+1wrMsCEqgqp1yhxQWCpQlgp8i0DXQrN42+u8P4ZssiE7SUn43YgWj2xWjCMYnx2OSDd9CakkKPYE39ztwj4l9DSPFlTFB
mBoj1YmFNlilB0L7YsrxHCE2nqV48Am9Hniq+3WL+yKsaSqTvpR5JjsYBMdaTd0mdliLemM/
CpCttylUlH5skSOXK6KEQJnFzlrj7e6sdmhow4+fcU4TDT+mHyA3pqzSqHnvlWHxHsqx8x0BRsbLlxye0uTlWeTHPRwh/ZS6/
iBfwL6ttbbGCiVSNuPcmlbOygKdlPdlewoEUyxlLEGSeA+tG65Cobk7AzbooArmclXEYNbAV0RKcZc/
k7gZs5OsZHHjegdicG2LJMwRLWsllKuSs3+9hRhV+EB9BdbxY13fpRfrT6zj2Z0lhiSixzqdfoog719u2O4Qf+8/+R0LSD1UAuNxln4p3KPZ9envz
WgX/AX6w79709pgkbnReA==

- The real m3u8 key hid in somewhere of a key file
- File name encrypted

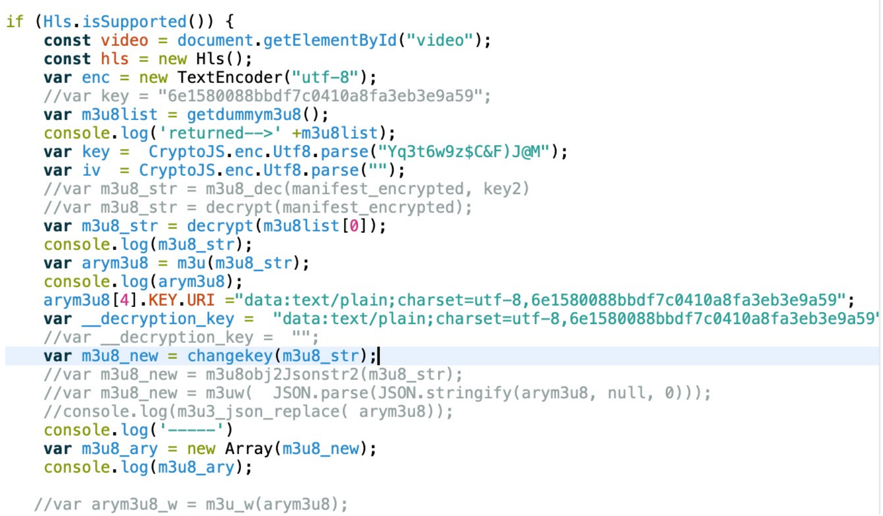
6e1580088bbdf7c0410a8fa3eb3e9a59

Mystified Key



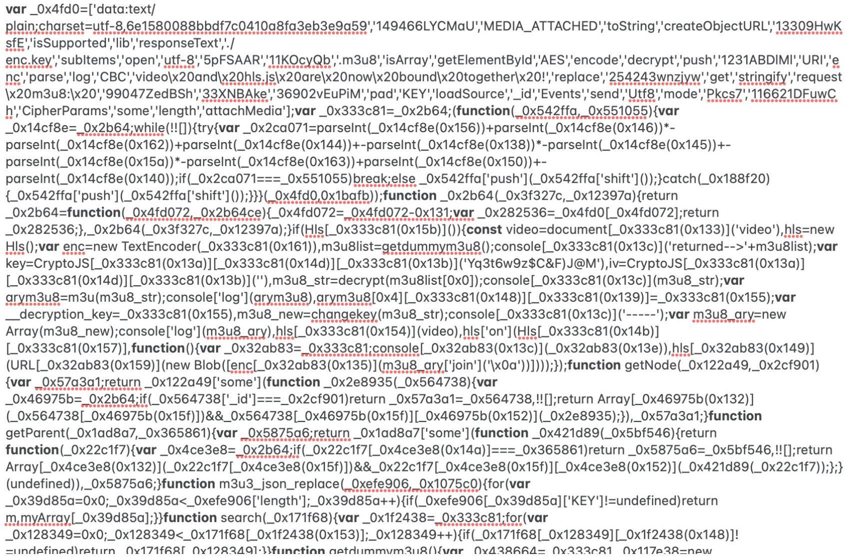
DdwL7yYNwP7MdYx0lgwJ1vFlMmP2Ktcj2jLD2Ujl4wYbRi4dJbuxccQ580RN/csGRO+jVpRTIEB
z3ppBLtEoJi1EwAAlcsicOAM7iYUrkcSV36mPVkUZLsd7EekSKMEkTHmPU3XKfyPEVuLwd9Iz9
R9fAE8fomKrAt0Y/J8cvs/6SeMrWO/UV/8Endk+W6gyZhTA/FiTUc/aGToKX4XBB0ZugeZ6xbg6v
XD6XzbCA3aTPM11u8lLv6WJuq90REfVvFxtXXAfJDFhsvByFpi6gK2Go6XZMeeC6WSkRFj6Q7b
yV6aW8aWF3cBADpmVznHSjLXqoVly1OqfGq/mG/Phf24alK96IF5WxH63Zgby2NKeM+tEPuoL
U90TPzu6NpuYYBhyl 6e1580088bbdf7c0410a8fa3eb3e9a59 j+uQz6yfVSMPc0vPDjb1QeW2Z
KjbLBK+ERYTlxlvJhEDpaYNl6w4st8vNNPAau3lkPhh8ZY=

Encrypted Javascrpt file



```
if (Hls.isSupported()) {
    const video = document.getElementById("video");
    const hls = new Hls();
    var enc = new TextEncoder("utf-8");
    //var key = "6e1580088bbdf7c0410a8fa3eb3e9a59";
    var m3u8list = getdummym3u8();
    console.log('returned-->' +m3u8list);
    var key =  CryptoJS.enc.Utf8.parse("Yq3t6w9z$C&F)J@M");
    var iv  = CryptoJS.enc.Utf8.parse("");
    //var m3u8_str = m3u8_dec(manifest_encrypted, key2)
    //var m3u8_str = decrypt(manifest_encrypted);
    var m3u8_str = decrypt(m3u8list[0]);
    console.log(m3u8_str);
    var arym3u8 = m3u(m3u8_str);
    console.log(arym3u8);
    arym3u8[4].KEY.URI ="data:text/plain;charset=utf-8,6e1580088bbdf7c0410a8fa3eb3e9a59";
    var __decryption_key =  "data:text/plain;charset=utf-8,6e1580088bbdf7c0410a8fa3eb3e9a59'
    //var __decryption_key =  "";
    var m3u8_new = changekey(m3u8_str);
    //var m3u8_new = m3u8obj2Jsonstr2(m3u8_str);
    //var m3u8_new = m3uw(  JSON.parse(JSON.stringify(arym3u8, null, 0)));
    //console.log(m3u3_json_replace( arym3u8));
    console.log('-----')
    var m3u8_ary = new Array(m3u8_new);
    console.log(m3u8_ary);

  //var arym3u8_w = m3u_w(arym3u8);
```



```
var _0x4fd0=['data:text/
plain;charset=utf-8,6e1580088bbdf7c0410a8fa3eb3e9a59','149466LYCMaU','MEDIA_ATTACHED','toString','createObjectURL','13309HwK
sfE','isSupported','lib','responseText','./
enc.key','subItems','open','utf-8','5pFSAAR','11KOcyQb','.m3u8','isArray','getElementById','AES','encode','decrypt','push','1231ABDIMI','URI','e
nc','parse','log','CBC','video\x20and\x20hls.js\x20are\x20now\x20bound\x20together\x20!','replace','254243wnzjyw','get','stringify','request
\x20m3u8:\x20','99047ZedBSh','33XNBAke','36902vEuPiM','pad','KEY','loadSource','_id','Events','send','Utf8','mode','Pkcs7','116621DFuwC
h','CipherParams','some','length','attachMedia'];var _0x333c81=_0x2b64;(function(_0x542ffa,_0x551055){var
_0x14cf8e=_0x2b64;while(!![]){try{var _0x2ca071=parseInt(_0x14cf8e(0x156))+parseInt(_0x14cf8e(0x146))*-
parseInt(_0x14cf8e(0x162))+parseInt(_0x14cf8e(0x144))+-parseInt(_0x14cf8e(0x138))*-parseInt(_0x14cf8e(0x145))+-
parseInt(_0x14cf8e(0x15a))*-parseInt(_0x14cf8e(0x163))+parseInt(_0x14cf8e(0x150))+-
parseInt(_0x14cf8e(0x140));if(_0x2ca071===_0x551055)break;else _0x542ffa['push'](_0x542ffa['shift']());}catch(_0x188f20)
{_0x542ffa['push'](_0x542ffa['shift']());}}}(_0x4fd0,0x1bafb));function _0x2b64(_0x3f327c,_0x12397a){return
_0x2b64=function(_0x4fd072,_0x2b64ce){_0x4fd072=_0x4fd072-0x131;var _0x282536=_0x4fd0[_0x4fd072];return
_0x282536;},_0x2b64(_0x3f327c,_0x12397a);}if(Hls[_0x333c81(0x15b)]()){const video=document[_0x333c81(0x133)]('video'),hls=new
Hls();var enc=new TextEncoder(_0x333c81(0x161)),m3u8list=getdummym3u8();console[_0x333c81(0x13c)]('returned-->'+m3u8list);var
key=CryptoJS[_0x333c81(0x13a)][_0x333c81(0x14d)][_0x333c81(0x13b)]('Yq3t6w9z$C&F)J@M'),iv=CryptoJS[_0x333c81(0x13a)]
[_0x333c81(0x14d)][_0x333c81(0x13b)](''),m3u8_str=decrypt(m3u8list[0x0]);console[_0x333c81(0x13c)](m3u8_str);var
arym3u8=m3u(m3u8_str);console['log'](arym3u8),arym3u8[0x4][_0x333c81(0x148)][_0x333c81(0x139)]=_0x333c81(0x155);var
__decryption_key=_0x333c81(0x155),m3u8_new=changekey(m3u8_str);console[_0x333c81(0x13c)]('-----');var m3u8_ary=new
Array(m3u8_new);console['log'](m3u8_ary),hls[_0x333c81(0x154)](video),hls['on'](Hls[_0x333c81(0x14b)]
[_0x333c81(0x157)],function(){var _0x32ab83=_0x333c81;console[_0x32ab83(0x13c)](_0x32ab83(0x13e)),hls[_0x32ab83(0x149)]
(URL[_0x32ab83(0x159)](new Blob([enc[_0x32ab83(0x135)](m3u8_ary['join']('\x0a'))])));});function getNode(_0x122a49,_0x2cf901)
{var _0x57a3a1;return _0x122a49['some'](function _0x2e8935(_0x564738){var
_0x46975b=_0x2b64;if(_0x564738['_id']===_0x2cf901)return _0x57a3a1=_0x564738,!![];return Array[_0x46975b(0x132)]
(_0x564738[_0x46975b(0x15f)])&&_0x564738[_0x46975b(0x15f)][_0x46975b(0x152)](_0x2e8935);}),_0x57a3a1;}function
getParent(_0x1ad8a7,_0x365861){var _0x5875a6;return _0x1ad8a7['some'](function _0x421d89(_0x5bf546){return
function(_0x22c1f7){var _0x4ce3e8=_0x2b64;if(_0x22c1f7[_0x4ce3e8(0x14a)]===_0x365861)return _0x5875a6=_0x5bf546,!![];return
Array[_0x4ce3e8(0x132)](_0x22c1f7[_0x4ce3e8(0x15f)])&&_0x22c1f7[_0x4ce3e8(0x15f)][_0x4ce3e8(0x152)](_0x421d89(_0x22c1f7));};}
(undefined)),_0x5875a6;}function m3u3_json_replace(_0xefe906,_0x1075c0){for(var
_0x39d85a=0x0;_0x39d85a<_0xefe906['length'];_0x39d85a++){if(_0xefe906[_0x39d85a]['KEY']!=undefined)return
m,myArray[_0x39d85a];}}function search(_0x171f68){var _0x1f2438=_0x333c81;for(var
_0x128349=0x0;_0x128349<_0x171f68[_0x1f2438(0x153)];_0x128349++){if(_0x171f68[_0x128349][_0x1f2438(0x148)]!
=undefined)return _0x171f68[_0x128349];}}function getdummym3u8(){var _0x438664=_0x333c81,_0x117e38=new
```

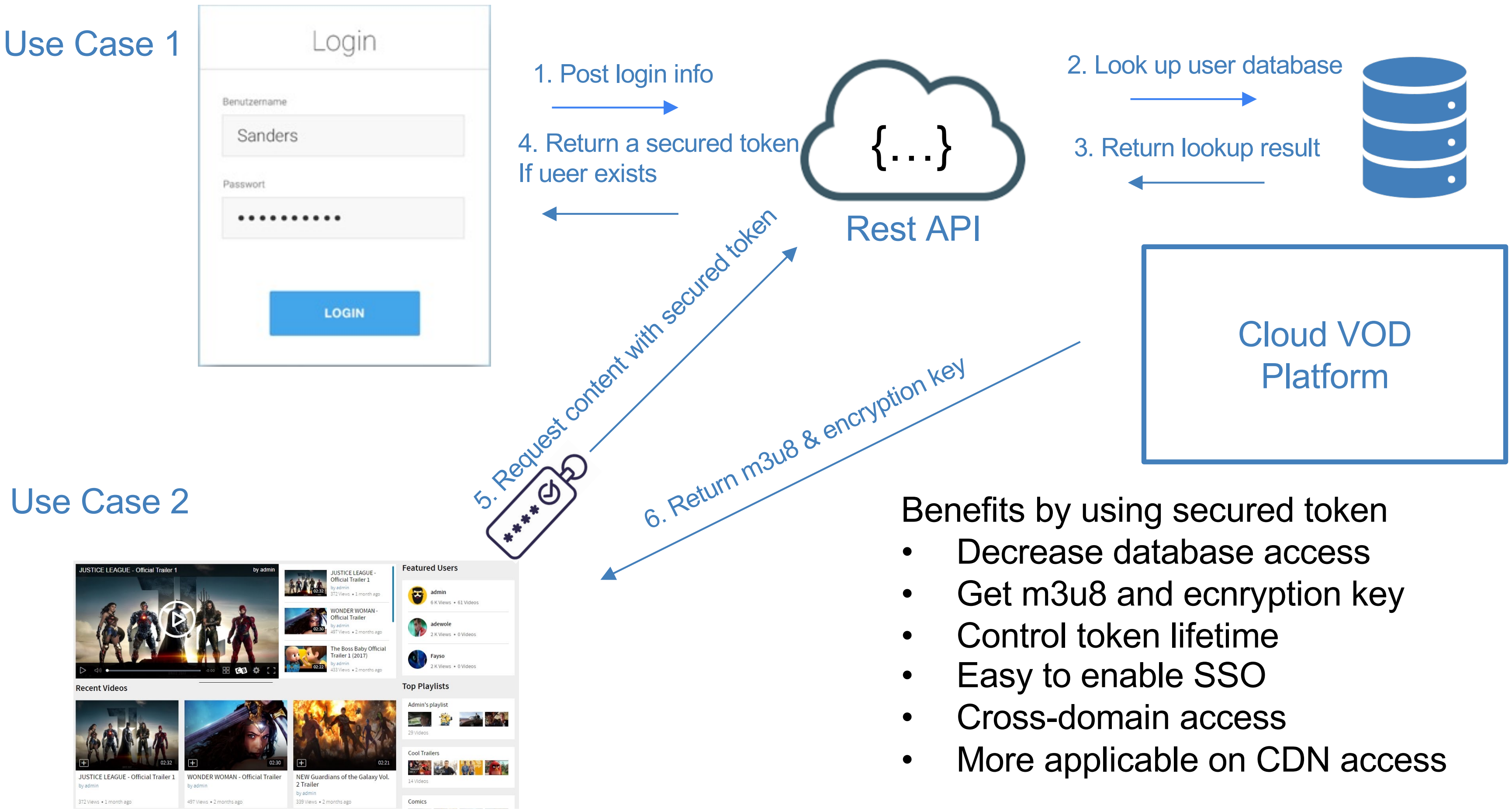
Pros

- **Encrypted javascript cannot be decrypted**
- Domain lock
- Debug protection
- Disable browser console output

Cons

- May cause performance low
- Non-browser sniffer tool like Wireshark can see all http requests and response
- Hard to maintain source and encrypted javascripts

Secured Token Authentication



Use Case 1

1. Post login info

2. Look up user database

3. Return lookup result

4. Return a secured token If ueer exists

Rest API

Cloud VOD Platform

Use Case 2

5. Request content with secured token

6. Return m3u8 & encryption key

Benefits by using secured token

- Decrease database access
- Get m3u8 and ecnryption key
- Control token lifetime
- Easy to enable SSO
- Cross-domain access
- More applicable on CDN access