*THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE*

# Solving BYOD Privacy Issues with Multi-Level Authenticated Encryption

**Surabhi Shukla**
M.E. Scholar, MPCT (Gwalior), RGPV (Bhopal), India
**Neelam Joshi**
Professor, MPCT (Gwalior), RGPV (Bhopal), India

***Abstract:***
*BYOD a term which is getting more attention now a day, this isn't new term. Many enterprises are using this technique from the last few decades, but now what's new in this and why is it getting so importance now? This question arises in mind of every IT tech user. Client now don't want itself to be bound anymore. Client needs its own freedom to work and the way by which it wants to work. Focusing this demand of client I have tried to propose a technique of BYOD with combination of cloud. Cloud; a storage space where we can store our data and can use anytime, anywhere according to our need. We aren't including any TPA here; all the responsibilities lay down on cloud server itself.*

## 1. Introduction

"Encryption is not enough"; the increase in web applications, cloud computing and SaaS offerings and the BYOD phenomenon are attracting employees, business partners and customers to increasingly access information on devices aren't managed by IT dept. this has resulted in security implications for data leakage, data theft and regulatory compliance. To protect valuable information, organizations must stop making a distinction between devices in the corporate network and devices outside of it.

## 2. Related Work

Many security solutions today are simply off the shelf data encryption. While a good start, the only way to fully ensure privacy is by authenticating the team members you communicate with. In case of BYOD we can use BYOE too. It depends totally on client that which type of encryption it wants to choose. In this approach of Authenticated Encryption, I am using AES 256 bit for encryption as well. Enterprises are trying to depend on BYOD with the basic networking technique, but I want to approach it with cloud; because cloud is beneficial future for tech era. As I am trying it initially on the cloud, so I am generating, 1-to-1 connection between client and server (cloud-based). Due to this 1-to-1 we don't need any service provider in the middle. That's why our data breach can be reduced to certain level. Endpoint encryption solution provides automatic, on-the-fly, enterprise-strength encryption to safeguard data regardless of where files and folders are stored. It's transparent, so employees can use their personal devices worry free.
So much work has been done for this; technicians and enterprise employee want to secure their data at any extreme level. As we all know that there are number of encryption algorithm to make our data safe from intruders. On all these algorithm's number of experiments has made to check their compatibility level with the given information. Now a day's concept of OTP is getting importance for the sake of security. As it provides two-factor authentication, which makes the authentication more secure from the previous techniques. According to TechTarget, Active Directory can no longer hold down the identity management services fort. You need cloud based authentication and identity services to step-in.

## 3. Theoretical Background

IT enterprises have already implemented full device security and management software for their agency owned devices and is expanding that paradigm to give network access to personal phones, tabs and other devices. In doing so, public sector organizations may focus more on security and less on end-user privacy. While security and privacy aren't mutually exclusive by any means, a predisposition towards one versus the other can lead public sector organizations down different paths.
It seems that many jurisdictions, we reviewed still struggle with employee privacy. By struggle, I mean that there is a lack of uniformity among policies across jurisdictions when it comes to handling privacy. Some states specifically call out the challenges of balancing security vs. privacy; others incorporate explicit caveats to privacy expectations. We also noticed that in some cases, the development of a policy seems to be separate and specific to the implementation of a program. Policies tend to rely heavily on guidelines while remaining more vague on the mechanics of implementation or leaving that decision up to those seeking to seize the opportunity.[Josh Heard; Marketing Manager AT&T; 5 Challenges for public sector BYOD]

a. SLA is a term which plays hard-core method to make your data secure enough. SLA is a contractual document between IT resource providers and consumer. Actually, it's an appropriate QoS (Quality of Service) for an individual application or any user in an IT system/enterprise.
b. OTP is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. It's based on HMAC SHA algorithm, which actually isn't encryption algorithm infect it's a hashing algorithm and this algorithm isn't reversible, which clearly means that you can't use the result to go back to the source.

*3.1. Problem Statement*

As cloud is a new emerging technique and is adapting via many enterprise very quickly. The reason behind this is very simple that it gives many benefits like cost saving, less operational time, etc. But as we know that good thing comes with some flaw in it. Cloud consist with the every time biggest flaw of network i.e. security. Security is a major issue for a long year back and so the cloud is facing the same too; but we have to differentiate between security and privacy first. I am trying to give privacy as much as I can.

*3.2. Proposed Framework*

BYOD (Bring Your Own Device) is a new technique which will be adopted by all the enterprise via 2020. So, I have approach this technique for our data security. Giving any new algorithm is a complexity task and can't found so much reliable. I have come up with an idea to mix two types of algorithm to make a strong enough wall to secure our data from attackers.
Combination of hashing algorithm (HMAC SHA) and AES (256 bits) will make a strong enough authentication and encrypted data. This concept will fulfill the security control with effect of privacy challenges too.

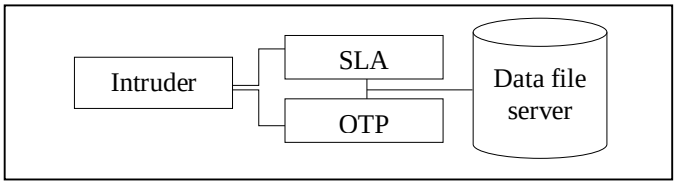


*Figure 1*

A. Working principle for the given technique –

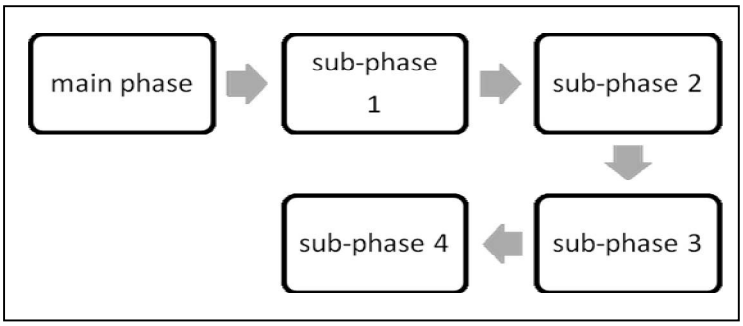


*Figure 2*

1. Main phase- requires login-id & password to enter
2. Sub-phase 1- select the operation, but can't operate
3. Sub-phase 2 – to perform the operation, user has to prove that's its authenticated.
4. Sub-phase 3- now can perform operation
5. Sub-phase 4- finally reach the server to access required file.

B. Proposed algorithm –

Figure 3

1. Initiate the server first.
2. If correct IP then proceed to step 3
   Else
   Move to step 1
3. Enter information on login page
4. If correct then proceed to step 5
   Else
   Move to step 3

Figure 4

5. { Select operation
6. { If operation is upload
7. Fetch the selected file & encrypt it.
8. Before uploading file the authenticated encryption will check
9. {If found correct client then step 10
10. File can be send to server
    Else
    Move to step 8
    }
    }

Figure 5

11. Else operation is download
12. Fetch the selected file
13. But before downloading, authentication will be required.
14. { If found correct then step 15
15. Easily decrypt file
    { Else
    Move to step 13
    }
    }
    }
16. Logout.

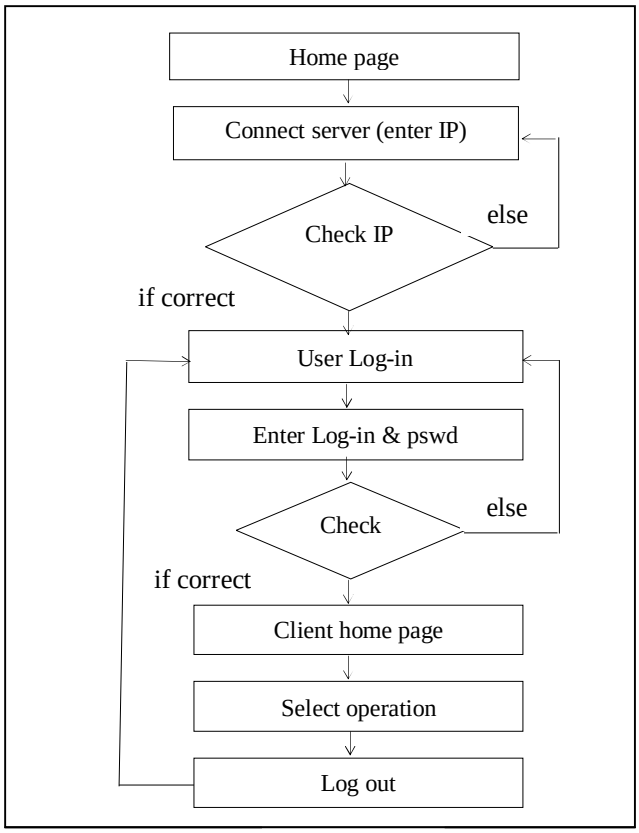


*Figure 3*

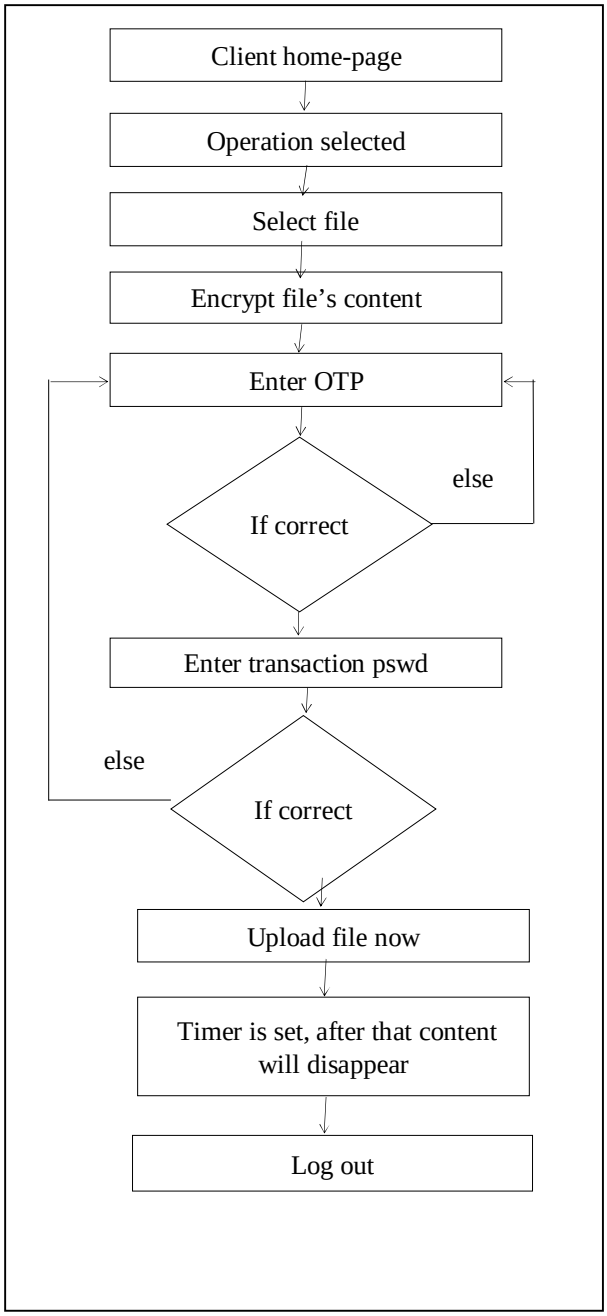


*Figure 4*

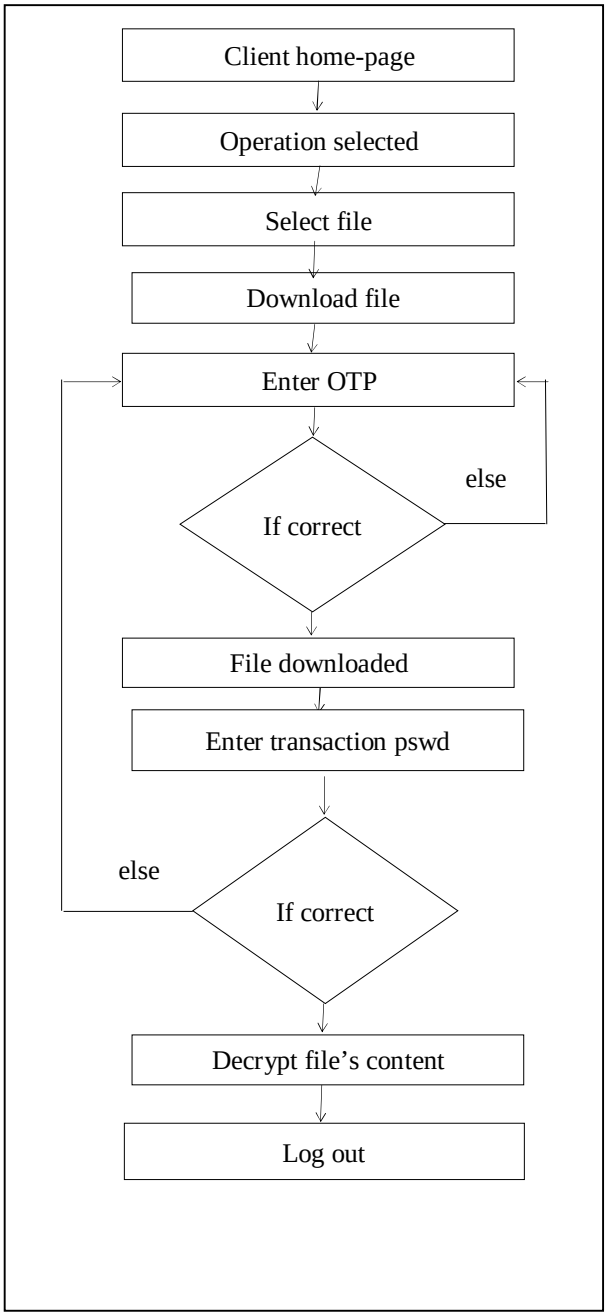


*Figure 5*


*Figure 6*


*Figure 7*

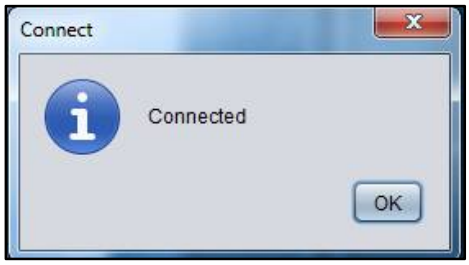


*Figure 8*


*Figure 9*

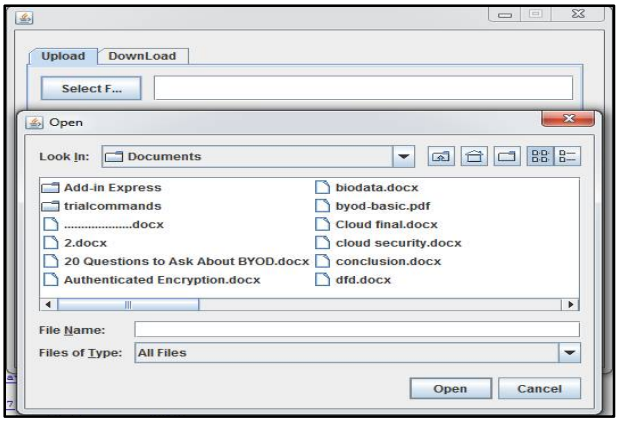


*Figure 10*

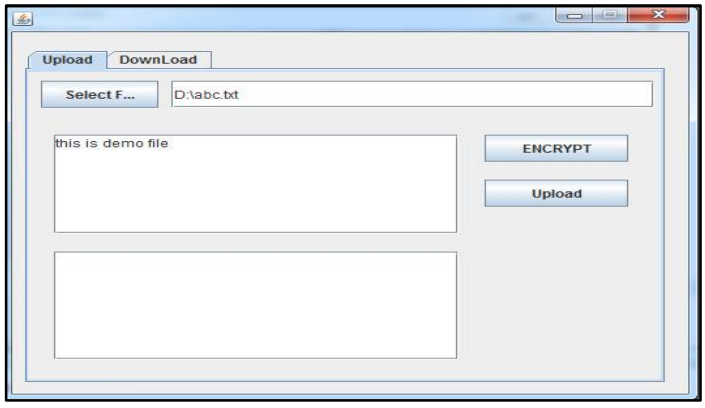


*Figure 11*

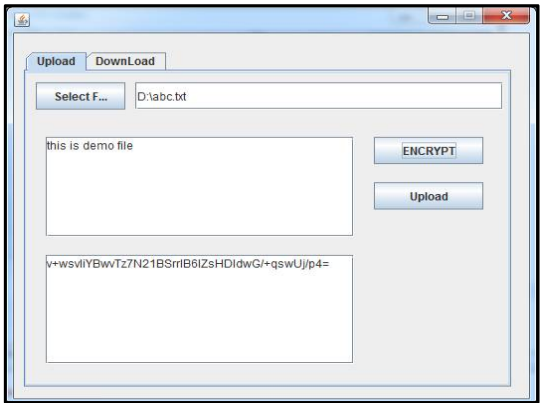


*Figure 12*


*Figure 13*

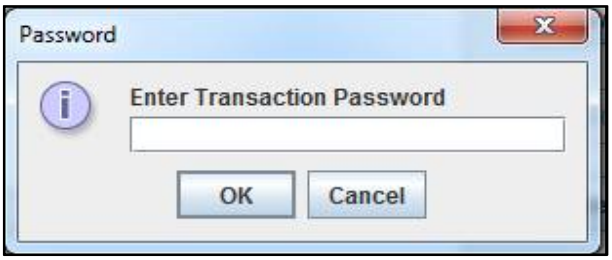


*Figure 14*

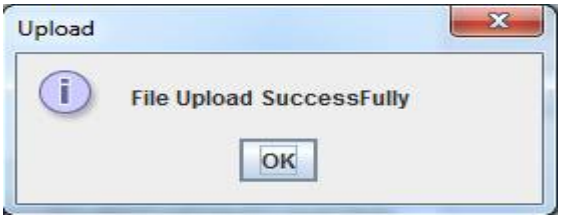


*Figure 15*

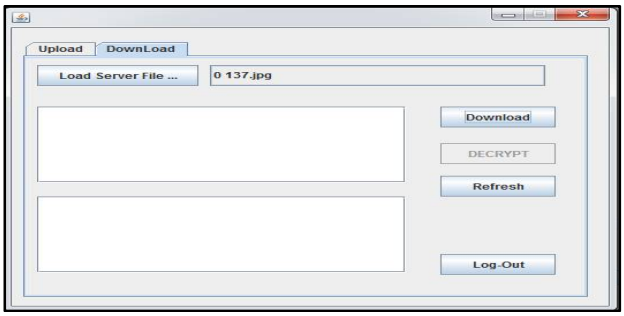


*Figure 16*

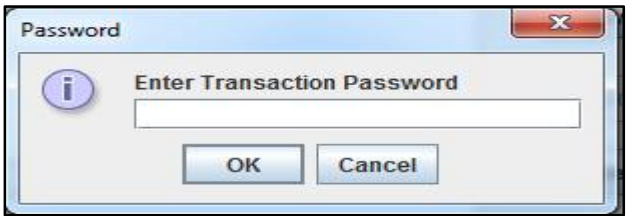


*Figure 17*


*Figure 18*

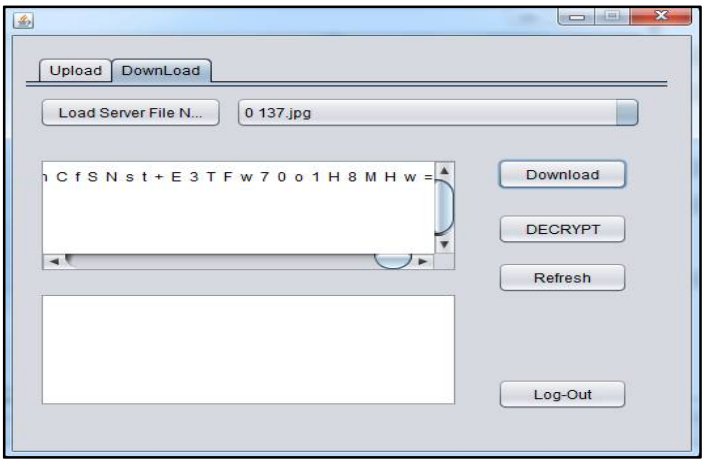


*Figure 19*

*3.3. Future Scope & Conclusion*

Research work is on a fast speed track in case of BYOD. Everyday enterprises are trying their best to provide a quality service to client. According to me security has taken a great concern for BYOD, but we should not neglect privacy in this case too. Privacy too is important as compared to security. According to my presented approach privacy has taken a concern. I have used authenticated encryption with and additional feature of multi-level authentication; this will increase a security level at some point.

But in case of this multi-level authenticated encryption I have reached at point of privacy of data but somewhere time has been a flaw in this case. Future work can be based on how to reduce time complexity here in case of big content data file. Future of IT enterprises will lay down here in BYOD with giving client the facility of BYOE.

**4. References**

i. www.techgig.com
ii. www.webopedia.com
iii. Josh Heard; Marketing Manager AT&T; 5 Challenges for public sector BYOD
iv. Surabhi Shukla;Public Cloud Security Challenges & Solutions;Volume 3 Issue 4, April 2015;IJSER15100.
v. "Cloud Computing Security Issues and Challenges";Kuyoro S. O., Ibikunle F., Awodele O.; International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011.
vi. Information Assurance Framework;2010
vii. BYOD with Multi-Factor Authentication;SurabhiShukla and Neelam Joshi; International Journal of Computer Sciences and Engineering Vol.-3(6), PP(104-107) June 2015, E-ISSN: 2347-2693
viii. D. Zissis, D. Lekkas / Future Generation Computer Systems 28 (2012) 583–592
ix. Clarke, N. L., and Furnell S. M. 2007. Advanced user authentication for mobile devices. Computers & security 26, no. 2: 109-119.