AUTHENTICATION USING MULTIPLE ENCRYPTION

BY

TUNIR CHAUDHURI (19BIT0212)

RAAVI SHIVA SESHI REDDY (19BIT0173)

OUR PROFESSOR,

JEYANTHI N

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

ABSTRACT

We live in an era where it is very difficult to achieve a task without taking help from technology, especially the internet. We need to use network and data so frequently in our day-to-day life that it becomes extremely important to keep our data safe. So, the fundamental concepts of privacy and security are taught in every educational institution of the world.

Information security is a general term that is used to refer to various segments of security, starting from threats, attacks to defence, protection and so on. Authentication is one such domain that offers a lot to be explored. But authentication is a vast concept, that covers a lot of ideas. If authentication can be combined with encryption, we can get a protection at a much better level than what already exists now.

This is the aim of our project. We intend to improve the existing system of user authentication using asymmetric encryption that will solve a number of issues which the current system fails to solve.

LITERATURE SURVEY

AUTHORS	**YEAR**	**TECHNOLOGY**	**MERITS**	**DEMERITS**
Nat Maysenburg, Ross Schulman	2020	Internet of Things	Helpful for sensitive data	Time consuming process
Andi Wilson Thompson	2020	Multi factor authentication	Supports any kind of data	Complex process
Brian Lennon	2015	Language understanding AI	Simple and cheap	Supports only selected languages
Steven N Peskind	2014	Protocol modification	Fast process	Supports only email accounts
Michael Silverstein	2016	Password length analysis	Cheap process	Works for simple passwords only
George Boone, Jonathan Huang, Tim Sweijs	2020	Biometrics analysis	Efficient security and privacy	Expensive process
Paul W Grimm	2014	Password analysis	Cheap and fast	Less efficiency, less accuracy
Ewa Stanczyk	2017	Photograph analysis	High efficiency	Expensive process
David A Scott	2016	Biometrics analysis	Fast process	Less efficiency, expensive process
Luciana Duranti, Allison Stanfield	2021	Multi factor authentication	Supports all kinds of users	Complex process
Simon Parkinson, Na Liu, Liam Grant	2020	Activity trackers	High efficiency, high accuracy	Works for limited types of data and limited users
Ran Gao, Huawei Tu	2021	Body movement, arm raising gesture	High efficiency, high accuracy	Works only for smartwatch

Karen Renaud, Antonella De Angeli	2014	Biometrics and visual data analysis	Fast process	Expensive process, less efficiency
Tsu Yang Wu, Yuh Min Tseng	2019	Password analysis	Cheap and efficient	Works for simple passwords only
Hung Yu Chien, Jinn Ke Jan	2013	Password length analysis	Cheap process	Works for simple passwords only, less efficiency
lt. Col. Jitender Paul Singh, Dr Mamata, Sunil Kumar	2015	Cloud computing	1.Not required to remember long passwords 2.Provides privacy and confidentially and non-repudiation by symmetric and asymmetric keys	Works for simple passwords and cloud applications
AL Zahra jo Mohammed, Ali. A. Yassin	2019	Iot authentication by multifactor authentication	Proposed protocol is safe and secure against well-known malicious attacks such as eavesdropping and traffic attacks	Designed only based on smart iot mobile devices, time consuming
Subhash Chandra,	2018	Access control using	Proposed	Lengthy

sumit Jaiswal, Ravi Shankar Singh, Jyothi Chauhan		Multifactor authentication in cloud	system and taken steps to implement and provide security was good	process and there can still be a chance of manipulation because of digital OTP generation
Riyadh Abdul Amir, Reham Mustafa, Hazem M.EI. bakry	2016	Authentication using identity detection	The idea of implementing the security by using iris detection is good and it provides some good security	In this methodology they have used only a single pattern of recognition using iris detection, however it is better to have some other options for authentication
Ehinome J. Ikhalia, Dr Chris O. Imafidon	2013	The need for two factor authentications in social media	1.Enchanced security 2.Reduces risk 3.Prevents monetary loss 4.Reduces identity theft 5.Reduces data theft 6.Increases flexibility	1.Costly 2.Inconvenient
Alexandra okada, Denise Whitlock, Wayne Holmes, Chris Edwards	2018	E-authentication for E - education	Strong building methodology for authenticat	Lengthy and costly

			ion in different basis.	
Heather Walker	2017	Digital identity-social media	1.Tokenization 2.Using Restful service end points to facilitate registration	Requires best method of strategy for user credentials security from third party authentication
CA Technologies	2015	CA advanced authentication	1.Reduces the risk of inappropriate access 2.Reduces the risk of employee identity theft 3.Reduces the fraudulent activity	2. Costly and inconvenient.
Aishwarya Mali, Chinmay Mahalle, Mihir Kulkarni, Tejas Nangude, Geeta Navale	2017	Digital authentication and verification on smart phones using CRIPT (cipher random integer procreation and translation) algorithm	Accuracy, efficiency for smart phone, simplicity is high	Security is not too strong, mentioned for mobile only
Sanjoli Single, Jasmeet Singh	2013	Cloud data using authentication and encryption technique	Provides strong security to data with both extensible authenticat	Lengthy process

			ion protocol and Rijndael encryption algorithm	
M.Yildirim, Mackie	2019	Improve password security and memorability	The proposed methods are good and efficient	Moderately difficult process
Aleksandr Ometov, Sergey Bezzateev, Niko Makitalo, Sergey Andreev, Tommi Mikkonen, Yevgeni Koucheryavy	2018	Survey: Multi factor authentication	Considering their survey password, token, voice, facial, ocular-based, finger print these authentication methods mostly possess higher – medium significance and behaviour, beam-forming, ocs, ecg, eeg, possess medium to low	1.Poor Task efficiency, age, cognitive abilities etc. 2.Poor probabilistic behaviour 3.Poor security 4.Poor integration 5.Poor robustness 6.Poor privacy

			significance and DNA, hand geometry, location, vein, thermal image are at medium	
Ganorkar, Vyawahare	2018	Graphical password analysis	User friendly and reduces the brute force, dictionary, spyware attacks	Involves in too lengthy process in both registration and as login proceeds
Kalaikavitha.E, Juliana Gnanaselvi	2013	Encrypted OPT	Good idea of implementing user login through mail reading without opt entering	Low accuracy, There may be a chance of third-party user access
Woong Go, Kwang Woo Lee, Jin Kwak	2014	Biometric analysis with password	Best way of designing the authentication process for strong secure and privacy	Very much complex

IDENTIFIED PROBLEMS

The existing system fails to provide a standard level of security. We have seen many times in the news channels and newspapers that several user accounts are being hacked, including accounts of big companies like Facebook, Google, etc. The traditional authentication technique is not enough to prevent modern hackers who use unauthorised methods to use these accounts. However illegal it may seem; we currently have no answer to this problem if we continue to use the conventional methods.

POSSIBLE SOLUTIONS

The best solution is to discontinue using traditional approach and try something new. Our encryption approach will be similar to Asymmetric encryption but it is not exactly the same. It can be used in the place of user authentication system to verify and validate the identity of the user in a more efficient way. This will have a strong encryption algorithm and it will be improved further by the policy of “password for password” method which will need the user to set a password for his own password. In other words, it resembles a method of double password but they are linked in such a way that only the correct user will get access to his/her account, and other users will not.

OUR ALGORITHM

Step 1: Declare c = 0, f1 = 0, z = 0, f = (actual first password), s = (actual second password)

Step 2: If c >= 3 go to step 5

Step 3: Accept first password (first)

Step 4: If first (with encryption and value of c) = f (with different encryption) then f1 = 1 and go to step 5

Otherwise z = z + 1 (and if z > 1 then c = c + 1) and go to step 2

Step 5: If f1 = 0 or c > 1 then exit

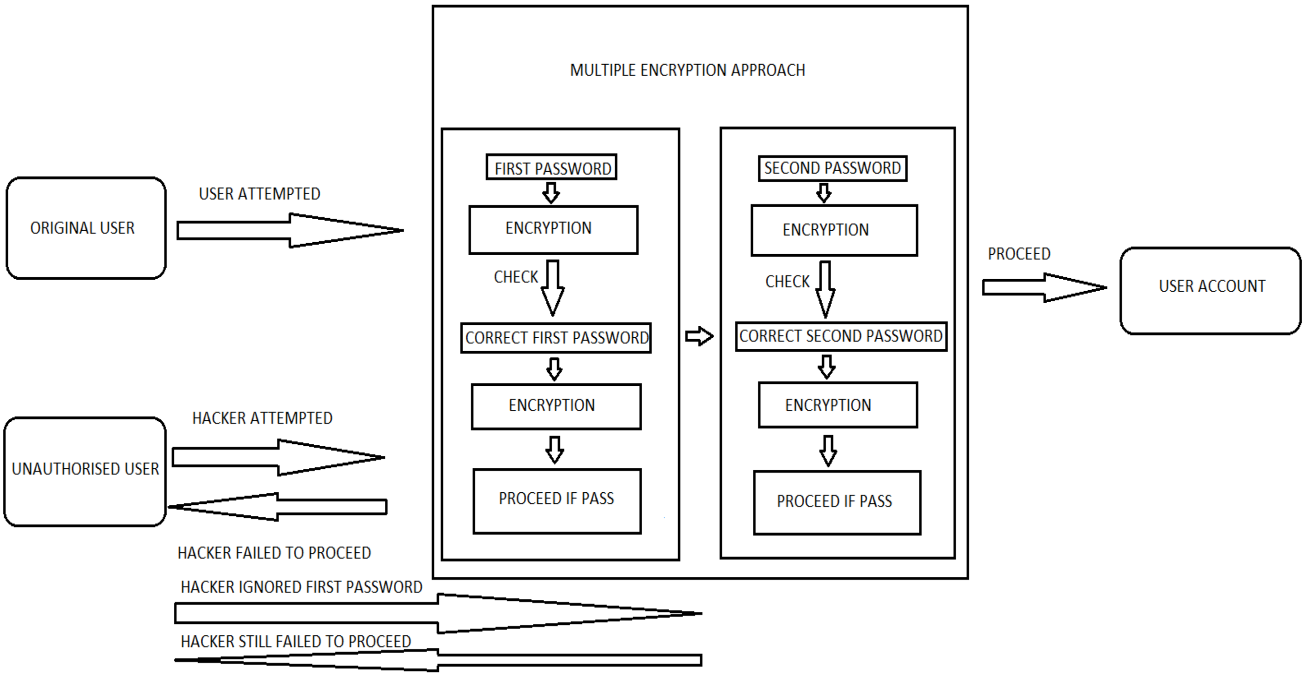
Step 6: Accept second password (second)

Step 7: If second (with different encryption, value of c, value of f1) = s (with another different encryption) then success

Otherwise exit

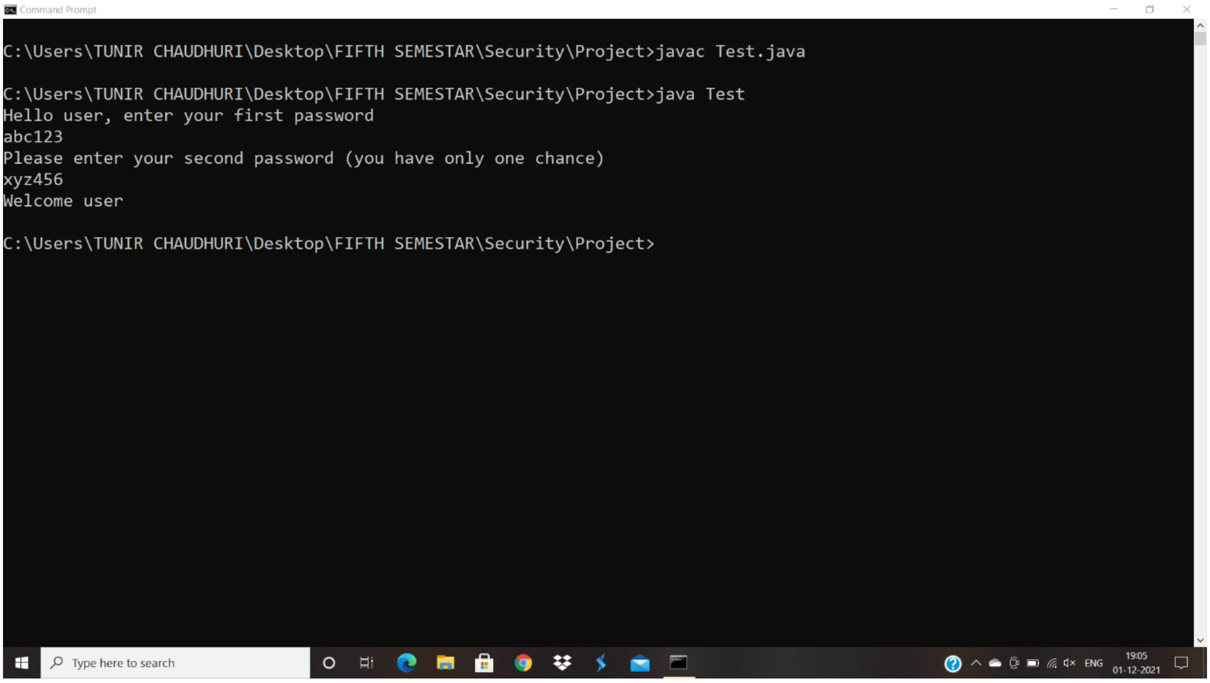
Step 8: If success, welcome user. If exit, report hacker.

ARCHITECTURE



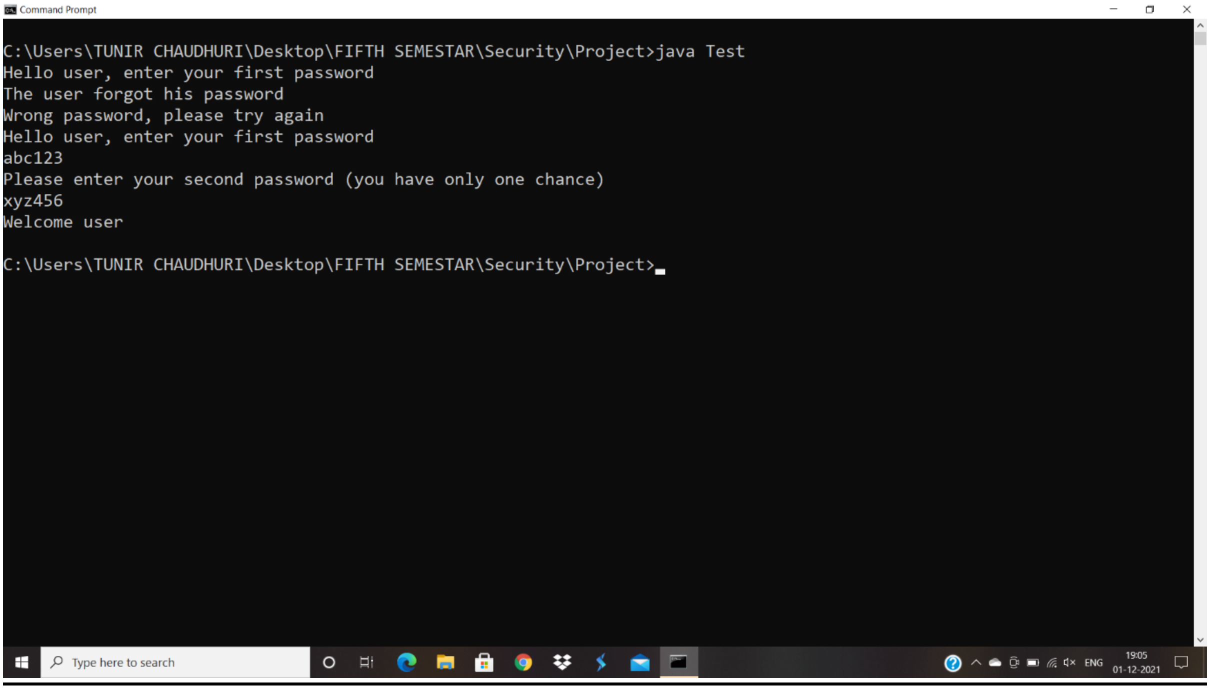
RESULTS

CASE 1: The user enters his password



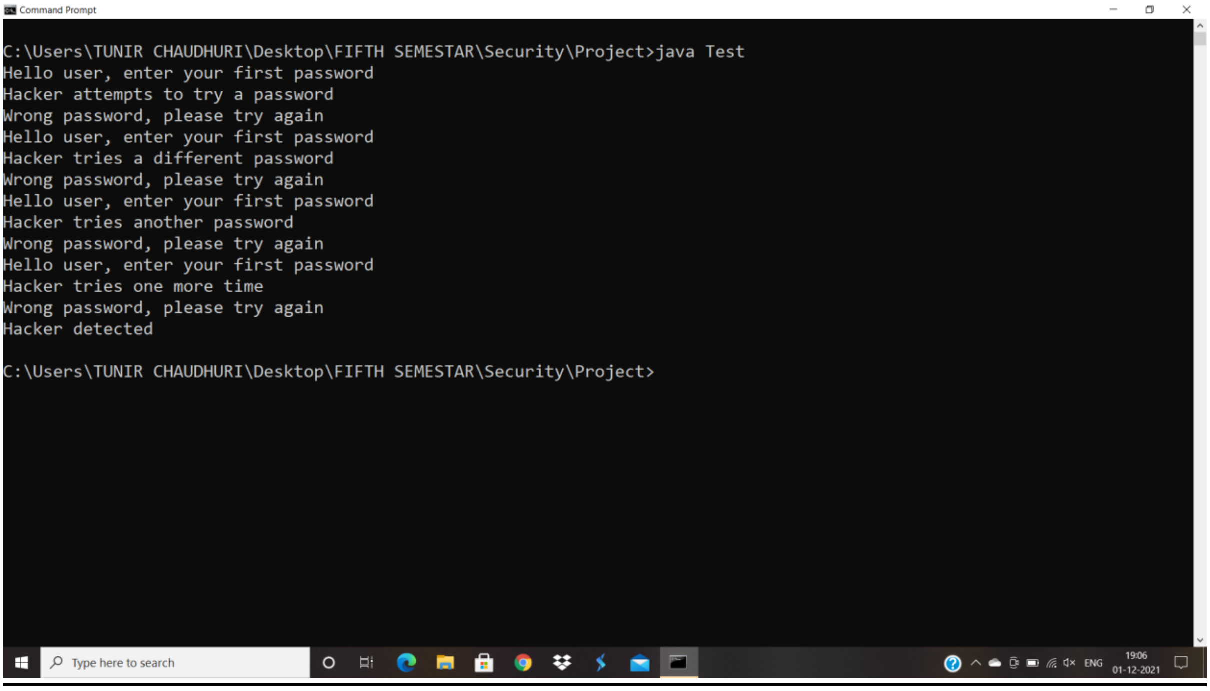
```
C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>javac Test.java

C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>java Test
Hello user, enter your first password
abc123
Please enter your second password (you have only one chance)
xyz456
Welcome user

C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>
```

CASE 2: The user forgets his password, then he remembers it



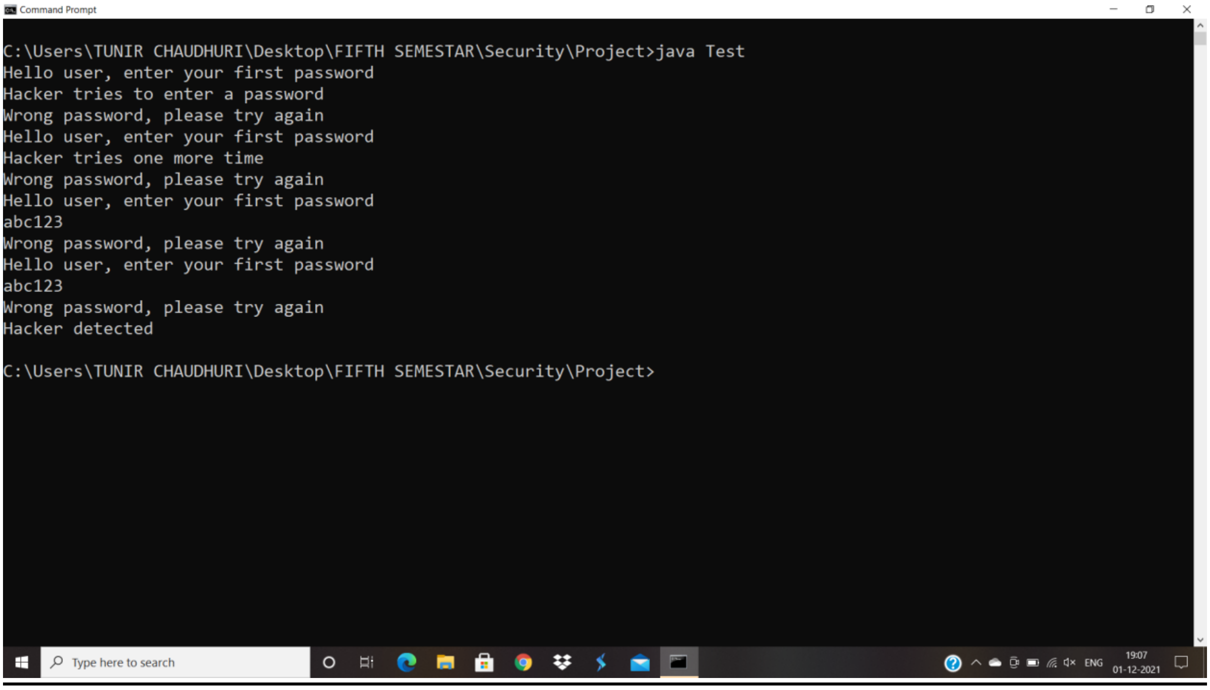
```
C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>java Test
Hello user, enter your first password
The user forgot his password
Wrong password, please try again
Hello user, enter your first password
abc123
Please enter your second password (you have only one chance)
xyz456
Welcome user

C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>
```

CASE 3: The hacker attempts to crack user’s password by guessing



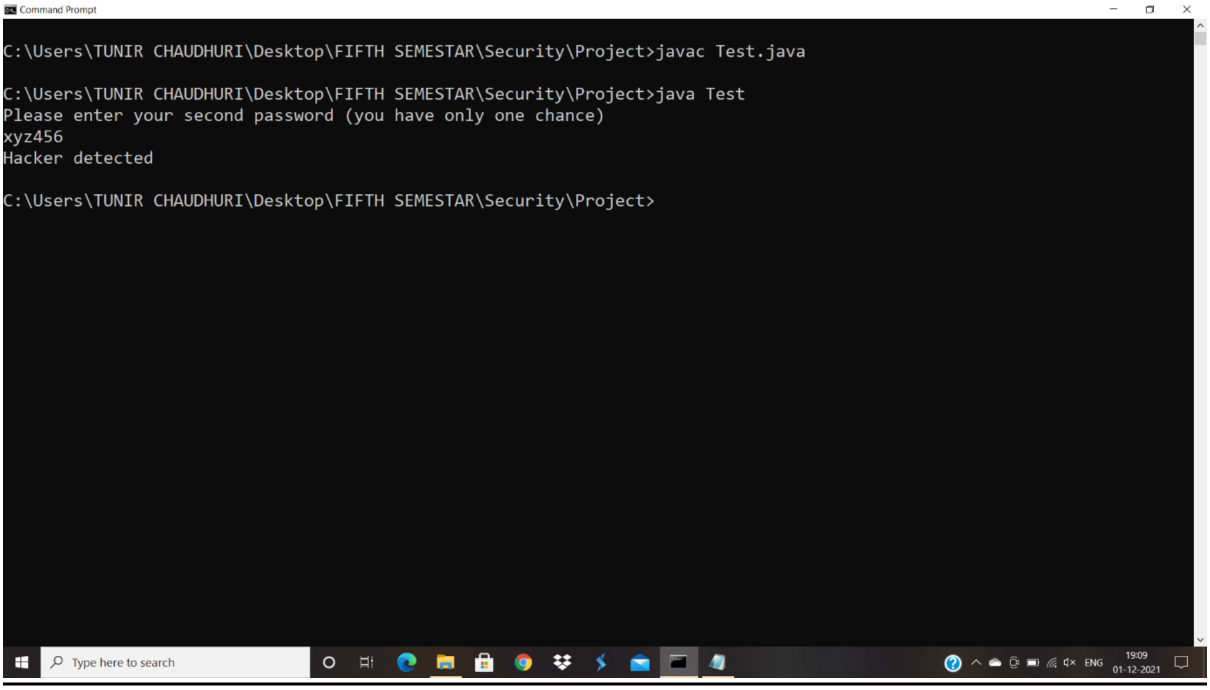
```
C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>java Test
Hello user, enter your first password
Hacker attempts to try a password
Wrong password, please try again
Hello user, enter your first password
Hacker tries a different password
Wrong password, please try again
Hello user, enter your first password
Hacker tries another password
Wrong password, please try again
Hello user, enter your first password
Hacker tries one more time
Wrong password, please try again
Hacker detected

C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>
```

CASE 4: The hacker attempts to crack user’s password and succeeds



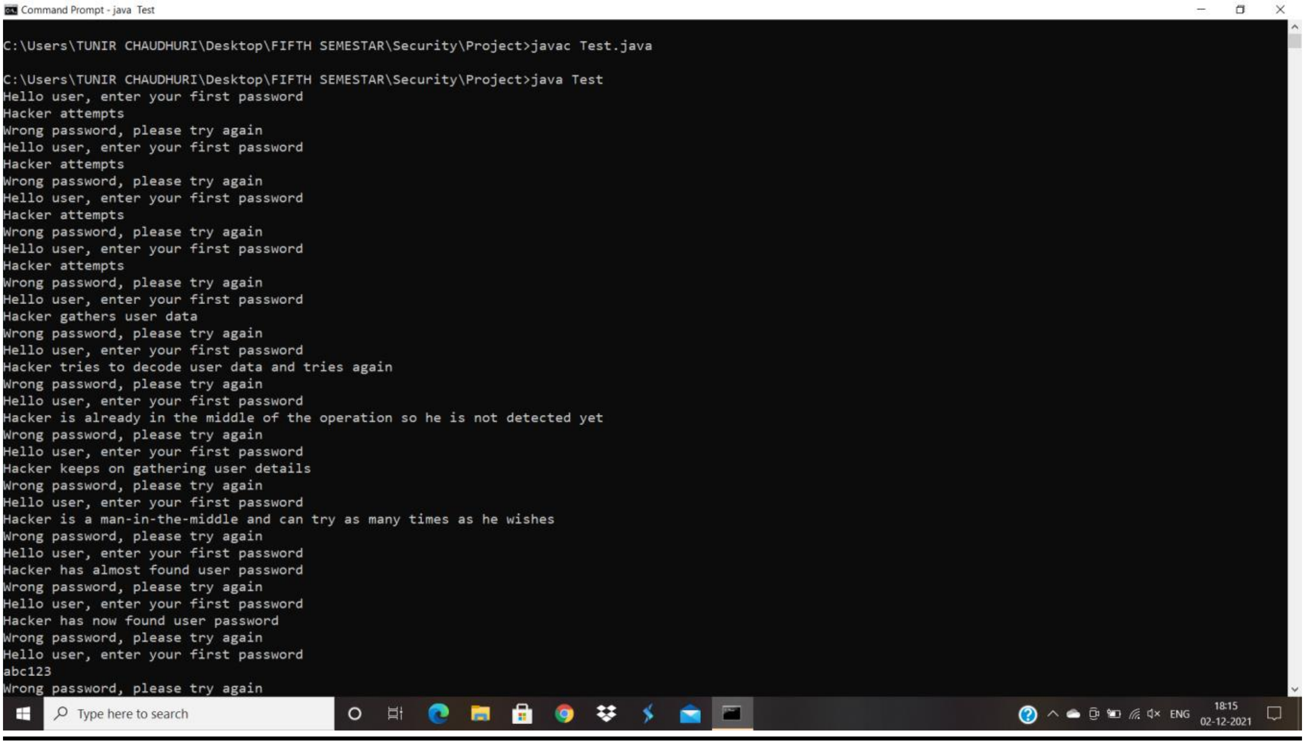
```
C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>java Test
Hello user, enter your first password
Hacker tries to enter a password
Wrong password, please try again
Hello user, enter your first password
Hacker tries one more time
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hacker detected

C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>
```

CASE 5: The hacker ignores first password by hacking

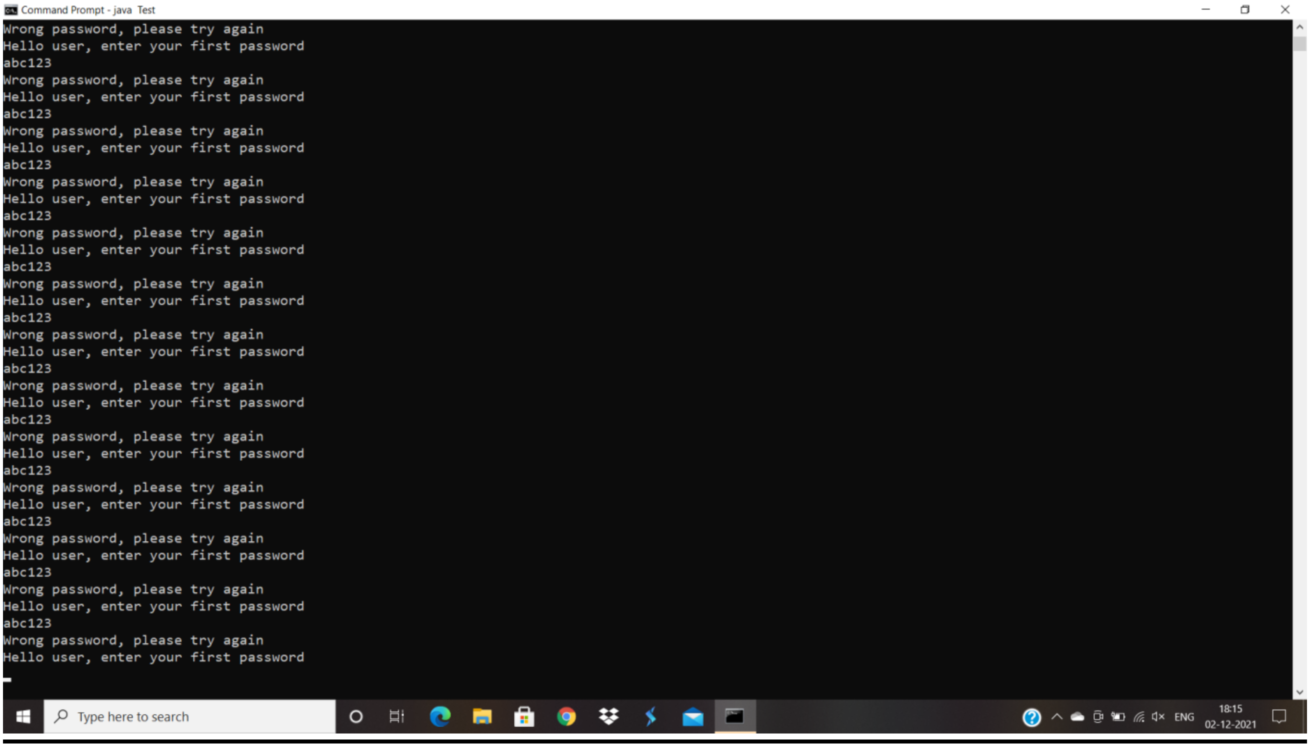


```
C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>javac Test.java

C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>java Test
Please enter your second password (you have only one chance)
xyz456
Hacker detected

C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>
```

CASE 6: The hacker is a man-in-the-middle who can stay undetected as he gathers user data to hack



```
C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>javac Test.java

C:\Users\TUNIR CHAUDHURI\Desktop\FIFTH SEMESTAR\Security\Project>java Test
Hello user, enter your first password
Hacker attempts
Wrong password, please try again
Hello user, enter your first password
Hacker attempts
Wrong password, please try again
Hello user, enter your first password
Hacker attempts
Wrong password, please try again
Hello user, enter your first password
Hacker attempts
Wrong password, please try again
Hello user, enter your first password
Hacker gathers user data
Wrong password, please try again
Hello user, enter your first password
Hacker tries to decode user data and tries again
Wrong password, please try again
Hello user, enter your first password
Hacker is already in the middle of the operation so he is not detected yet
Wrong password, please try again
Hello user, enter your first password
Hacker keeps on gathering user details
Wrong password, please try again
Hello user, enter your first password
Hacker is a man-in-the-middle and can try as many times as he wishes
Wrong password, please try again
Hello user, enter your first password
Hacker has almost found user password
Wrong password, please try again
Hello user, enter your first password
Hacker has now found user password
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
```



```
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
abc123
Wrong password, please try again
Hello user, enter your first password
_
```

In our algorithm, even if the hacker attempts trial and error method to guess the user's password, he cannot succeed. In all the above cases, the hacker failed to proceed even when he could find the user's password through unauthorised methods or ignore the first password layer in the above model or staying in an infinite trap of loop and eventually being reported if he decides to be a man-in-the-middle.

CONCLUSION

We have enjoyed working with our algorithm, and we hope that our project can contribute to the improvement in security of current models. We would like to implement our project at a bigger level in future. As there is always scope for improvement, we hope we can improve our model as we keep working in this field.

REFERENCES

https://www.researchgate.net/

https://www.jstor.org/

https://www.kaggle.com/

https://en.wikipedia.org/wiki/Password

https://en.wikipedia.org/wiki/Encryption

https://docs.oracle.com/javase/tutorial/