ICIC Express Letters
Volume **12**, Number **10**, October **2018**

ICIC International ©2018 ISSN 1881-803X
pp. 1061–1069

TEST PLAN SPECIFICATION USING SECURITY ATTRIBUTES: A DESIGN PERSPECTIVE

Mohd Waris Khan[1], Dhirendra Pandey[1] and Suhel Ahmad Khan[2]

[1]Department of Information and Technology
Babasaheb Bhimrao Ambedkar University (A Central University)
Vidya Vihar, Raebareli Road, Lucknow 226025, India
wariskhan070@gmail.com

[2]Department of Computer Science
Indira Gandhi National Tribal University, Amarkantak
Amarkantak, Madhya Pradesh 484887, India

Received January 2018; accepted April 2018

Abstract. *The increasing number of users of the Internet has created an environment where software plays a crucial role in all kinds of information exchange. This leads to increased demand of different type software and their respective uses in conducting all types of information interaction. The role of software is very important for any application/organization; hence its security cannot be neglected in any way. Security testing is an activity that exposes whether the security functions are accurately implemented, and whether software behaves correctly in the presence of a malicious attack. Making software secure is not only related to safety and confidentiality of a system that contain important or personal data, but it is also essential for giving better results. Therefore, testing of software is vital before it is being implemented in real-life systems. Security testing is performed at various phases of the software life cycle, starting from requirements definition and analysis, through design, implementation and verification. Finally, this paper points out future focus and development directions of the security testing profile. In this paper, we discuss various security attributes related to the software test plan specification, which are – authentication, authorization, confidentiality, availability, integrity, non-repudiation and resilience.*

Keywords: Security testing, Testing profile, Authentication, Authorization, Confidentiality, Availability, Integrity, Non-repudiation, Resilience

1. **Introduction.** Software security deficiencies do not come to surface as easily as other faults and errors found during testing. Therefore, software security testing is required to identify defects and faults that are rather difficult to make out. The security testing is performed to make sure that the software under test is satisfactorily robust and works in an adequate mode even at the time of a malicious attack [1,2]. Compound systems are hard to test and therefore the probabilities of getting untested portions are found. These untested portions act as loopholes through which a breach could be made in the software which may affect the efficiency and capability of software and may also result in loss of important information. To overcome such types of problems extended security testing profile needs to be developed, which may help to identify and address different types of security breach in the design phase of the software development life cycle. To perform these functions the main role is played by the security attributes of the test plan specification.

The main aim of software security testing is to make sure that sufficient attention is given to the software to identify the security risks and perform reasonable tests to ensure the proper functioning of the applied security measures. It also ensures that plenty of

DOI: 10.24507/icicel.12.10.1061

expertise exists to carry out adequate software security testing. It is one of the activities that are used to reduce vulnerabilities within a software system and control potential future costs. This signifies the testing of software security adherence to its function as well as non-functional constraints.

2. **Process Flow Diagram of Security Attributes in Test Plan Specification with Respect to Security Testing Profile.** Security testing is an important issue to make sure that our software is reliable and secure. The attributes of software security testing are correlated with security test plan specification with explanation. The security testing profile is purely dependent on all the parameters of test plan specification [1]. In Figure 1, it is clear that all security attributes are the parts of security test plan specification and play a vital role in the development of the security testing profile. STP gives developers an understanding and overview, i.e., whether the security requirements are consummated or not, and which vulnerability class is present in the software (the test object). As results traced from the use of security attributes explained through Figure 1 given below developers may conclude facts regarding the security quality of the software. In addition, it increases the security specific knowledge of the developers in means of how software vulnerabilities may be exploited (i.e., thinking like an attacker), which further makes them more aware of software security next time they develop software.

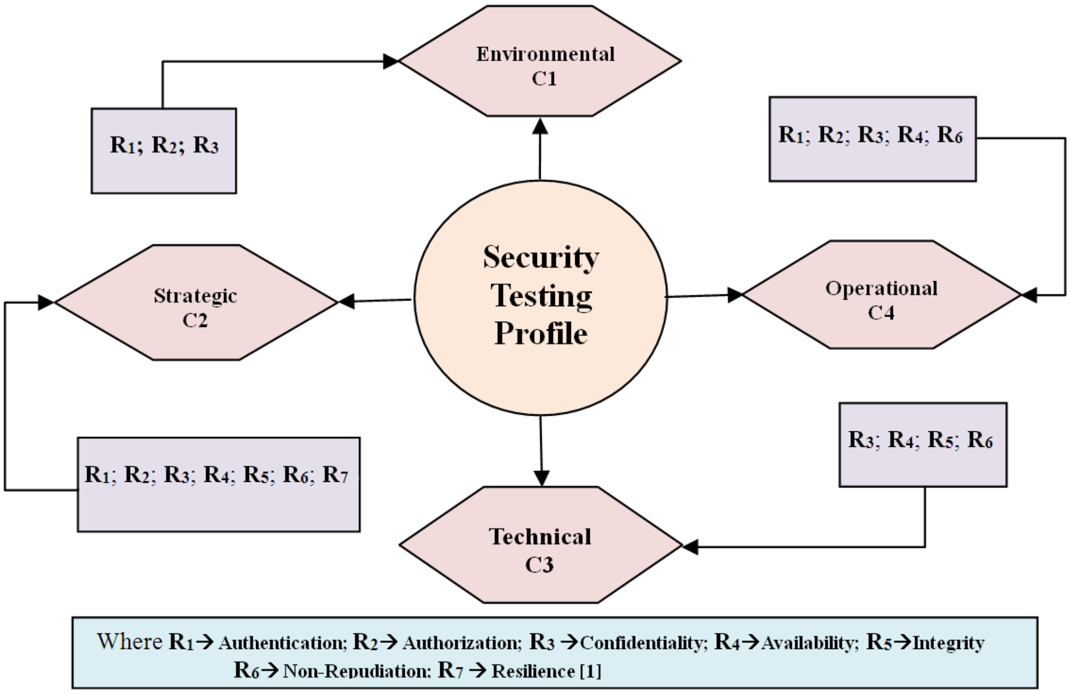
Environmental
C1
R1; R2; R3
R1; R2; R3; R4; R6
Strategic
C2
Security Testing Profile
Operational
C4
R1; R2; R3; R4; R5; R6; R7
R3; R4; R5; R6
Technical
C3
Where R1→ Authentication; R2→ Authorization; R3 →Confidentiality; R4→Availability; R5→Integrity
R6→ Non-Repudiation; R7 → Resilience [1]

Figure 1. Mapping of security testing attributes with test plan specification: STP perspective

2.1. **Environmental specification: R1, R2 and R3.** Identification of a right user/person before accessing the system is essential for any organization/system. The most important thing is that when an authentication check is passed only then the users are eligible to access the system information. Since the test environment includes the physical characteristics of the facilities like hardware, communications and system software, mode of usage/interface and other software or supplies, it signifies that environmental specification is affected through the attributes of the software security, i.e., R1, R2 and R3 [1,3].

2.2. **Strategic specification: R1, R2, R3, R4, R5, R6 and R7.** Strategic specification is the heart of the test plan, and should contain a description of how software security testing will be performed and elucidate issues that have a major impact on the success of testing and ultimately on the running project [1]. The completion criteria for the overall test plan will be set in advance in strategic specification [4]. Hence, it is required to set some benchmark or prepare a checklist at each phase to know whether the testing phase is complete or not. Therefore, in this case checklist is used for all the security attributes which are lying under the strategic test plan specification.

2.3. **Technical specification: R3, R4, R5 and R6.** In the test plan specification, the major issue is to select the appropriate tools and automation for specific problems. By selecting proper tools it may help in the development of software and ease the task of testing staff. In order to choose the right tool, it is important that requirements are formulated for the selection and use of the tool [1,5]. There may be no one tool of a definite type that fulfills all the requirements. Different potential users of the tool may also have different needs. Therefore, it may be possible that more than one of the same kinds of tools may be selected, and it is expected that software application must be tested in different platforms. Hence, it also indicates that Confidentiality (R3), Availability (R4), Integrity (R5) and Non-Repudiation (R6) are made effective.

2.4. **Operational specification: R1, R2, R3, R4 and R6.** In this process all the selected numbers of test cases are executed and the result is observed. The result of each test case must be recorded. If the testing is automated, the tool will record both the input and the respective results. Although, preparation and planning for security test operation occur throughout the software development life cycle, the operation itself typically occurs at the end of the software development life cycle [1,6]. As the result of operational specification the major by-products that come under these are test incident report, test logs, testing status & result, etc. Test environment, test cases/procedures, test data, etc. are checked which signifies that R1, R2, R3, R4 and R6 attributes of the security are affected.

There are two major purposes of planning for software security testing. The first purpose includes identification of items to be tested, testing task to be performed, personnel responsible for each task and the risks associated with the plan. The second purpose of planning is to develop the scope, approach, resources and schedule of the testing activity. Table 1 describes the effect of security testing attributes on test plan specification.

3. Use Cases for Example ATM System.

In Figure 2, example of use case of an ATM system and the functions of various security attributes are described. The role of security attributes with respect to test plan specification shed light on various stages, required to complete the process effectively [2,9]. This process also explicates that security attributes are the component of the test plan specification and plays a crucial role while designing the security testing profile (STP).

3.1. **Stage 1: System startup.** An interface between the system and the operator is established when the operator commands the system to startup as shown in Figure 3. The operator will check the amount of cash available in the cash dispenser. It requires primarily the authentication and authorization of the operator to use the system. In return the system first identifies the operator and then checks the level of clearance that the operator enjoys regarding to the limit of use of the system [2]. To complete this process, the role of confidentiality (R3) and availability (R4) comes into picture as part of the security attributes working on this phase along with R1 and R2 [2,9]. Any interface between the system and the operator will lie under the environmental as well as strategic

Table 1. Description of security testing attributes that affect security test plan specification at various levels of software development

S. No	Security Test Plan Specification	Security Testing Attributes that affect Test Plan Specification	Description
1.	Environmental C1	R1; R2; R3	• User's identification is checked for authentication [1]. • Define the permissions & restriction to specific user group or granting/revoking the privileges for the users.
2.	Strategic C2	R1; R2; R3; R4; R5; R6; R7	• Check interface for unauthorized and less privileged users. • Mirroring of data at the time of recovery. • Checked information may not be altered during the transit. • Tracking who access the systems and check its completeness means confirmation sent by receiver to sender (e.g., digital confirmation) [1,5]. • Check the resistance of the system to against attacks which can be implemented using encryption (e.g., OTP) [6].
3.	Technical C3	R3; R4; R5; R6	• Selection of appropriate tools to ensure that information and services are available to the intended users [1,2,9]. • Digital confirmation serves as acknowledgment that helps to validate both sender and receiver are genuine.
4.	Operational C4	R1; R2; R3; R4; R6	• Check test data, test procedures, test plan, test strategy, etc. • The confidentiality of information is maintained and it is displayed only to the genuine users of the system [1]. • Automation and test case provide a parallel platform regarding the availability of the system to the users when demanded [4,7]. • Confirmation sent by the receiver to the sender by means of digital certificates [8,9].

test plan specifications. In addition, mainstream and alternate scenario use cases of system startup process are described in Table 2.

3.2. **Stage 2: System shutdown.** In the second stage when the system is shutdown the connection of the ATM with the bank is severed. Here also the system first authenticates and authorizes the operator to shut down the system that is shown in Figure 4. The system's ability to authenticate and authorize the operator to shut down the system is based on the allotted unique ID of the operator specified by the bank. The system

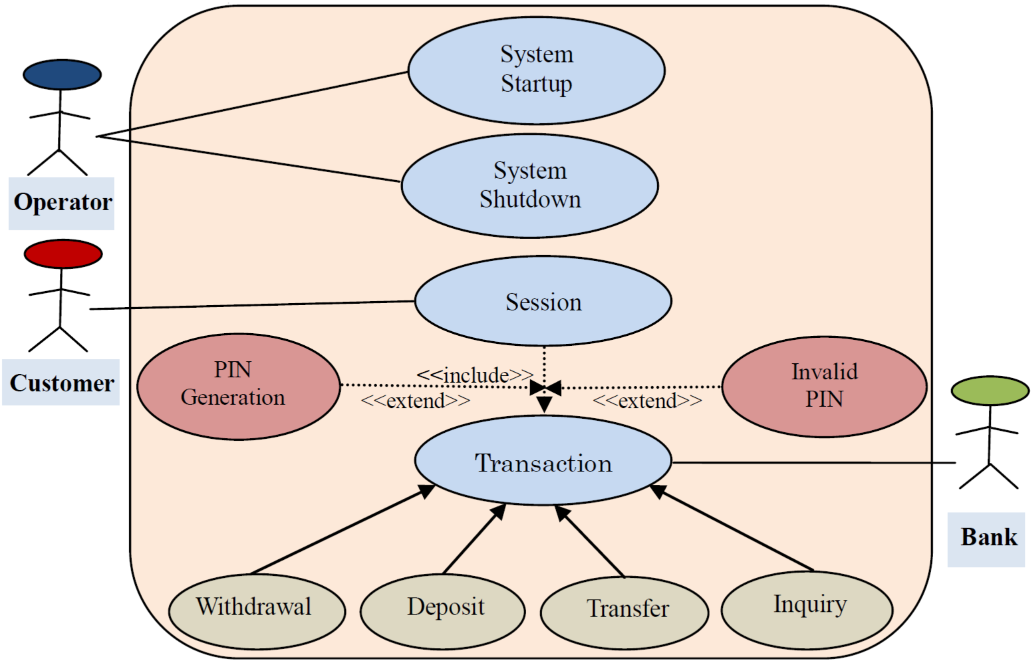

Figure 2. Use cases for example ATM system

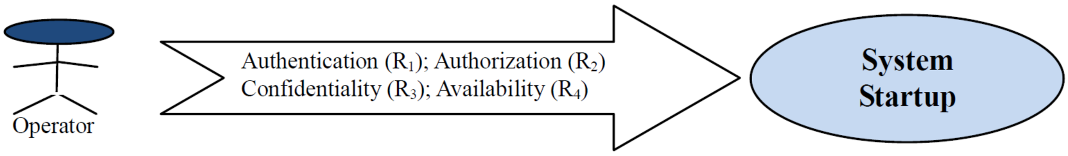
Operator
Authentication (R1); Authorization (R2)
Confidentiality (R3); Availability (R4)
System Startup

Figure 3. System startup process

Table 2. Mainstream and alternate scenarios of system startup process

Test Case(s)	Steps	Expected Results
Test Case	System Startup Process (Normal work-flow)	
1	Power Supply Open	The system will prompt for PIN.
2	The operator will enter PIN	The system will display the limited access as per required for an operator.
Test Case	System Startup Process (Alternate work-flow)	
1	Power Supply Open	The system will prompt for PIN.
2	Enter an invalid PIN	The system will display the limited access as per required for an operator.

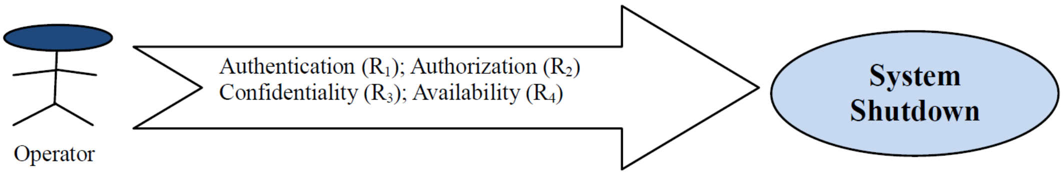
Operator
Authentication (R1); Authorization (R2)
Confidentiality (R3); Availability (R4)
System Shutdown

Figure 4. System shutdown process

Table 3. Mainstream and alternate scenarios of system shutdown process

Test Case(s)	Steps	Expected Results
Test Case	System Startup Process (Normal work-flow)	
1	Power Supply OFF	The system will prompt for PIN.
2	The operator will enter PIN	The system will logout first and then shutdown.
Test Case	System Startup Process (Alternate work-flow)	
1	Power Supply OFF	The system will prompt for PIN.
2	Enter an invalid PIN	The system will stay ON and display an error message.

verifies this ID which is a part of the security attribute related to confidentiality [2,9]. The security attributes working here are R1, R2, R3 and R4 (i.e., both environmental and strategic test plan specification). Further, Table 3 describes the mainstream and an alternate scenario of the system shutdown process.

3.3. **Stage 3: Session process.** In the third stage the interface between the customer and system is described known as a session. The session includes all the activities when a transaction is made between bank and customer. These activities including withdrawal, deposit, transfer, inquiry, PIN generation and change, changing the contact details, etc., are explained in Figure 5. Transaction also includes the process of identification and verification of the customer ID (ATM card details) through the process of confidential PIN provided to the customer from the bank. A session begins when the customer inserts the ATM card in the machine for making a transaction with bank. The machine then reads the card and asks the customer to enter the PIN to check the confidentiality of the customer via ATM card and PIN which authenticate the customer to make transaction [1,2]. If the PIN is invalid, the system rejects the authorization of the customer, hence confidentiality attribute of the user fails as the system does not recognize the authority of the user to make any transaction. In this phase R1 and R2 security attributes are affected in respect to environmental test plan specification [9]. If the system rejects the user's request due to invalid PIN, the session is closed and the system gets ready for a new session. In the same scenario, if the customers select the PIN generation option, then all the security attributes (R1 to R7) are used for different purposes followed by test plan specification. Additionally, Table 4 has shown the scenarios happen during the session process.

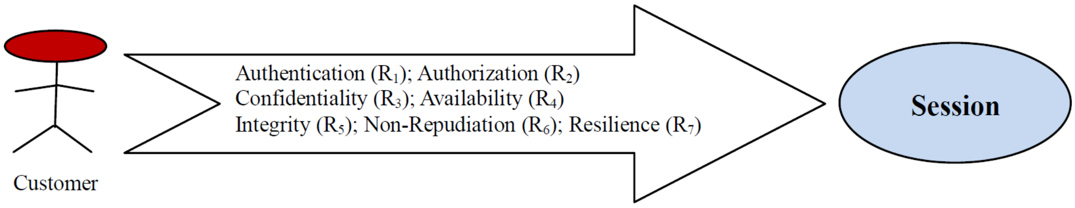
Customer
Authentication (R_1); Authorization (R_2)
Confidentiality (R_3); Availability (R_4)
Integrity (R_5); Non-Repudiation (R_6); Resilience (R_7)
Session

Figure 5. Session process

3.4. **Stage 4: Transaction process.** In the fourth stage, i.e., transaction use case is started within the session when the customer is authorized by the system after which customer chooses the type of transaction from the transaction menu to be performed by the system [2]. The type of transactions can be withdrawal, transfer, deposit, inquiry

TABLE 4. Mainstream and alternate scenarios for session established between users and a system

Test Case(s)	Steps	Expected Results
Test Case	Session: 1 (Normal work-flow)	
1	Insert Debit Card	The system will prompt for PIN.
2	Enter Valid PIN	The system will display a menu of transaction types.
3	System allows customers to perform a transaction	After performing successful transaction, the system asks whether customer wants another transaction.
4	System allows multiple transactions in one session if the customer answer is YES	The system will display a menu of transaction types.
5	Session ends when customer chooses not to do another transaction	System ejects cards and is ready to start a new session.
Test Case	Session: 1 (Alternate work-flow)	
1	Insert Debit Card	The system will prompt for PIN.
2	Enter an Invalid PIN	The system will return the card.
Test Case	Repeat Step: 1 of Session	
1	Select the option to "Cancel"	The system will return the card.
2	Repeat Steps: 1-4 of mainstream scenario and then customer selects the option to "Cancel"	The system will return the card.

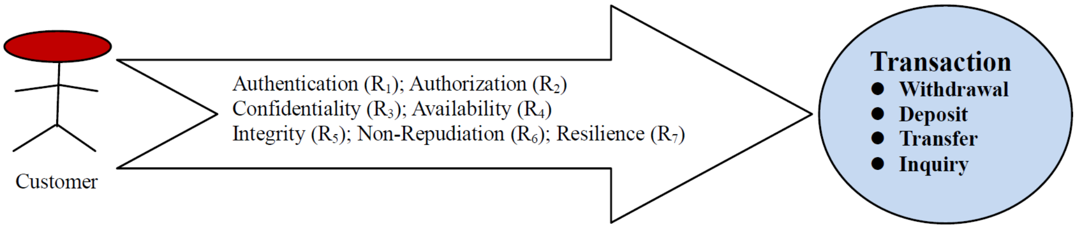
Customer
Authentication (R_1); Authorization (R_2)
Confidentiality (R_3); Availability (R_4)
Integrity (R_5); Non-Repudiation (R_6); Resilience (R_7)
Transaction
Withdrawal
Deposit
Transfer
Inquiry

FIGURE 6. Transaction process

and other banking services as shown in Figure 6. The customer is required to enter the correct PIN in order to qualify to transact. If the bank approves the transaction, the customer is permitted to avail the type of transaction from the ATM as he/she wishes. If the transaction is cancelled by the customer, or fails due to any other reasons other than repeated entries of invalid PIN, a screen will be displayed informing the customer of the reason for the failure of the transaction or if a customer may cancel the transaction by pressing the Cancel key then the system will reach at its initial stage.

In this process, all the security attributes (R1 to R7) are used for different purposes followed by test plan specification. R1 and R2 are identified only after which customer can make use of the cash dispenser. An interface is established between the customer and system where the system check to what limit the customer is permitted by the bank to withdraw the cash (use of R3, i.e., confidentiality between the user and the bank). The system then allows the customer to withdraw cash within the specified limit if not then the transaction declines [2,9]. In this case the system will select the appropriate tools for various banking services and then make those services available to the customer. In case

Table 5. Mainstream and alternate scenarios of transaction (withdrawal)

Test Case(s)	Steps	Expected Results
Test Case	Cash Withdrawal-1 (Normal work-flow)	
1	Insert Debit Card	The system will prompt for PIN.
2	Enter Valid PIN	The system will display the option to "Withdraw Cash".
3	Select the option to Withdrawal transaction	System displays a menu of account types.
4	Select the option from menu of account types	The system will prompt for an amount.
5	Enter valid amount that the system currently has and which in not more than the A/c balance.	The system will dispense the cash amount and offers customer the option of choosing to do another transaction or not.
6	If customer opted yes option, the system is displaying menu of account types	Repeat Steps 3 and 4. After successful transaction the system will return the card.
Test Case	Cash Withdrawal-2: Invalid PIN (Alternate work-flow)	
1	Repeat Step 1 of Cash Withdrawal-1	
2	Enter an invalid PIN	The system will return the card.
Test Case	Cash Withdrawal-3: Invalid Account Type	
1	Repeat Steps 1, 2 and 3 of Cash Withdrawal-1	
2	Select Invalid Account Type	The system will display an error message and system will return the card.
Test Case	Cash Withdrawal-4: Invalid Amount	
1	Repeat Steps 1 to 4) of Cash Withdrawal-1 with exceed amount (daily limit)	The system will display an error message and prompt for another amount.
2	Repeat Steps 1 to 4) of Cash Withdrawal-1 with 0 Rs. Or such amount that was not accepted	The system will display an error message and prompt for another amount.
3	Repeat Steps 1 to 4) of Cash Withdrawal-1 with valid amount	The system will dispense the cash amount and offers customer the option of choosing to do another transaction or not.
4	After choosing YES option and then customer select the option to "Cancel"	The system will return the card.
Test Case	Cash Withdrawal-5: Transaction Declined	
1	Repeat Steps 1 to 4) of Cash Withdrawal-1 with greater than account balance (invalid amount)	The system will return the card.
Test Case	Cash Withdrawal-6: Cancel Transaction	
1	Repeat Step 1 of Cash Withdrawal-1	
2	Select the option to "Cancel"	The system will return the card.
3	Repeat Steps 1 and 2 of Cash Withdrawal-1	
4	Select the option to "Cancel"	The system will return the card.
5	Repeat Steps 1, 2 and 3 of Cash Withdrawal-1	
6	Select the option to "Cancel"	The system will return the card.
7	Repeat Step from 1 to 4 of Cash Withdrawal-1	
8	Select the option to "Cancel"	The system will return the card.

of invalid PIN entry more than a specified time the system locks out the card for a specific duration of time to prevent any fraudulent activity. The system sends a message to the registered mobile number of the customer so as to notify the customer that an invalid attempt has been made to access his bank account and at a specific location which has been failed by the system. The security attribute R7 plays the role and commence this operation. Finally, Table 5 shows mainstream and alternate scenarios of transaction dealing with the withdrawal.

Similarly, all the use cases come under the ATM system are prepared. Hence, from the above description it can be concluded that all the security attributes have their own importance for different goals in different use cases.

4. **Conclusions.**

An essential security attribute of the test plan specification improves the security, dependency and the life of the software. During the development of STP the mentioned security attributes should be taken under consideration so as to reduce the chances of system failure and malicious attacks. The proposed work gives a view that the security attributes will collaborate with test plan specification to make the software system more durable and resilient by creating security testing profile. Future work will concentrate on developing a framework for integrating security requirements for STP, by using security attributes with the test plan specification. Further, the documentation will be done followed by its implementation into the life cycle stages to achieve maximum security standards at all the stages of software development.

REFERENCES

[1] M. W. Khan, D. Pandey and S. A. Khan, Critical review on software testing: Security perspective, *Smart Trends in Information Technology and Computer Communications in Springer CCIS Series, SmartCom 2016*, Jaipur, India, pp.714-723, 2016.

[2] *http://www.mathcs.gordon.edu/courses/cs211/ATMExample/UseCases.html.*

[3] D. P. Gilliam, T. L. Wolfe, J. S. Sherif and M. Bishop, Software security checklist for the software life cycle, *Proc. of the 12th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp.243-248, 2003.

[4] D. Zhang, C. Nie and B. Xu, A Markov decision approach to optimize testing profile in software testing, *The 9th International Conference for Young Scientists*, pp.1205-1209, 2008.

[5] S. A. Khan and R. A. Khan, Software security testing process, *Recent Trends in Computing and Communication*, pp.38-42, 2013.

[6] I. Schieferdecker, J. Grossmann and M. Schneider, Model-based security testing, *Workshop on Model-Based Testing, EPTCS*, vol.80, pp.1-12, 2012.

[7] R. Kumar, S. A. Khan and R. A. Khan, Durability challenges in software engineering, *The Journal of Defense Software Engineering*, pp.29-31, 2016.

[8] H. Chen and J. P. Corriveau, Security testing and compliance for online banking in real-world, *Proc. of International Multi Conference of Engineers and Computer Scientists*, Hong Kong, 2009.

[9] T.-Y. Gu, Y.-S. Shi and Y.-Y. Fang, Research on software security testing, *World Academy of Science, Engineering and Technology*, pp.647-651, 2010.