A New Approach of Authentication in E-commerce Transaction to Reduce the Effect of MITM Attack

Rupali Savita¹, Prof. Unmukh Datta²
¹PG student, CSE, MPCT, Gwalior, India
²Associate Professor, Deptt. of CSE, MPCT, Gwalior, India

Abstract—In proposed work author has focused on Two ways Authentication-(client and server) which provides Advanced Security for Rapid and Highly secure Communication. A discussion has been done in this study about E-commerce, Web Services, Principle of Security, Authentication, and MITM attack. This process involves Authentication which provides Availability, Reliability, and Security in communication and removes the MITM attack. Authentications are identical and prevent the users to unauthorized access of data and information. This paper explains different types of authentication consequences, techniques under different circumstances as well. MITM attack is used widely as a method of attacking the network. Proposed technique provides better security and performance in the presence of MITM attack in comparison of conventional Two way (client and server) authentication, the result shows the advantages of proposed work.

Keywords—MITM attack, authentication, web service, phishing, Security.

I. INTRODUCTION

Nowadays E-commerce has become the real achievement of the time for Electronic Business. It means managing in Products and Administrations through the Electronic Media and Web. On the Web, it communicates to a website of the merchant, who trades, produces or open facilities to the client from the gateway using a digital shopping cart or digital shopping basket scheme and allows payment through credit card, debit card or Electronic fund transfer (EFT) [1].

Favourable position of E-Business
- Lack of street movement, labour and page work,
- We can control immense expenses,
- E-Business can build deals,
- It can make items and administrations accessible in remote ranges,
- E-Business gives 24X7 provision and facilities.

II. WEBSITE SECURITY

The Network service is a brand-new circulated computational model utilizing the Service Oriented Architect (SOA), which composes the three basic operations. The three members are the SP (Service Provider), the SR (Service Requester) and the SB (Service Broker). Including three straightforward actions publishing, searching and Binding [2]. The structure of the Service Oriented Architect of web service is shown in Figure 1.

![Service oriented architect](image)

Fig1. Service oriented architect [2]

A. Security specification in web service

The Web Services Security (WS-Security) is most approved and comprehensive. It integrates the normally accepted security representations, contrivance and methodological provisions. The main aim of Web Services Security is to confirm the inclusiveness and concealment of the information processing with AP (application programs) by WS (web services) and to recommend the message header an extension of the Service Oriented Architect. The WS-Security joins differing security models, arrangements (configurations) and procedure (technique). It is one of the services concerned with standard terms.
B. Client side security issues

Client-side security is usually communication services with regard to the user. It may also require server verification and non-repudiation of receipt. In addition, various applications may anonymously browse on the Web. The submission of encryption is to deliver validation and privacy of online connections. Robust cryptography makes available the basis for attaining access control, operation permit, information integrity and responsibility.

C. Server side security issues

In the point of view of SP (service providers) security in general, server-side is the major concern for requiring proper client authentication and authorization, non-repudiation, sender un-recoverability (e.g., unspecified publishing on the Web), assessment trail and accountability, and also dependability and accessibility.

D. Transaction security issues

This is correspondingly significant for combining the consumer and the SP (service provider) side. Transaction anonymity includes many security facilities, information authentication, access control, information confidentiality, information integrity, and non-repudiation services and so on.

III. AIMS OF SECURITY

In a model world, we make certain the security reason, if each qualified module get each message proposed for it. There are the four leaders of security. Three more get to control, accessibility and freshness of information [3] [4].

A. Data Confidentiality

Authentication safeguards the dependability of the message by recognizing its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets.

B. Data Authentication

Security principle helps to verify the identity of a person. The authentication process makes clear in your mind the sender message or document is accurately made out. Authentications of data, is to verify the identity of the sender and receiver.

C. Data Integrity

The integrity principle protects data in opposition to active threats.

D. Data Non-repudiation

This helps to secure communication clients and sender can prove that the receiver can receive the message.

E. Data Access control

Access point enables contact between Host application and field devices, which controls the access point.

F. Data Availability

This is helping to provide the necessary needs of customer information.

G. Data Freshness

The principle of freshness means the receivers are receiving the fresh and latest data and make certain that no adversary can replay on not getting any younger data.

H. Scalability

Scalability is not directly connecting with security, but it is an important issue because it has a scalable security mechanism to handle large network.

IV. TECHNIQUES OF AUTHENTICATION

The guideline of security is to recognize a man or a PC framework that should be trusted [6]. Authentication is the confirmation which builds up the character of the client, which is permits client access to the resources. In software engineering, verification of a man’s personality is frequently needed to secure access to private information or frameworks.

A. Token based authentication

The token is a greatly valuable distinct option for a secret word. Token generates pseudo-random numbers. There is a little device that produces new variable each time it is utilized. This is protected by a secret key or PIN. Just when this pin has been entered one time password be created. Existing confirmation systems includes three fundamental "components": Something the client knows (e.g., secret key, PIN), something the client has (e.g., digital card) and something the client is (e.g., bio-metric trademark, for example, unique fingerprint recognition) [5].

One factor authentication: This confirmation component includes one factor (such as passwords).
Two factor authentication: This acquires the two components, which includes the gathering to be verified concerned with components [9] e.g. ATM machine. This figure demonstrate something you have (card, key) with something you know (secret word) to confirm a man.

Multi factor authentication: MFA, to be totally straightforward, is a layer term that depicts verification that uses two or more independent sources to set up and check the identity [7].

a. Something you have
b. Something you know
c. Something you are

It is based upon structures with typically two-factor confirmation. Since customers are using portable devices new and additional for banking and shopping, however, physical and logical security concerns have converged.

This, in turn, has formed more interest in three-factor authentication. This is protected and extremely serviceable. These procedures includes a novel method based on Transaction ID (identification) Code and SMS to enforce an additional security level with the old-style (traditional) Login/password scheme.

Multi factor authentication: MFA

B. Biometric Authentication

As we realize that word "Bio" has importance of life and "metric" has reason for mean measurement (estimation), we learn about program identification, which make utilization of the target or behavioural quality and that is called biometrics [1]:

1. Voice recognition
2. Hand geometry
3. Face recognition
4. Eye print for case retina and iris scans.
5. DNA
6. Fingerprint recognition etc.

Biometric security is concerned with the affirmation of confidentiality, honesty (integrity) and accessibility of data in all structures. Flow diagram is shown below in figure 5. Scans exchange people's biometric element (like fingerprints, etc.) into digital codes or numerical data that can be recorded in a database. Like facial recognition software, fingerprint scanning matches a person's code beside an access DB (database) of codes in organizing to verify that individual's personality (identity).
C. Captcha

Captcha mean “Completely Automated Public Turing test to tell the computer and human apart”. This is wholly computerized public test to make the Computer and human apart require human to write words or number to form distorted picture [6].

VI. MITM (MAN IN THE MIDDLE ATTACK)

In this segment current and relaxed security is studied and proposed against MITM attacks [8] [9]. All that take part in the MITM attack are (i) User (U), (ii) Service Provider (SP), (iii) fake Service Provider (SP’), Suppose that the U has attempted a connection to a web site SP’ which impersonates SP. SP’ is a man in the middle, i.e., SP’ connects to SP as well as U. Since the SP’ which connects to SP in order appended to the request, (Figure. 7) it contains the characteristics information on SP (e.g., URL information). This info is displayed to U who is expected to make sure whether it is as same as the connected party-SP’.

Man-in-the-middle attacks, assailant locales between the sender and receiver and sniffs any data being sent between two nodes. At times, the aggressor may imitate the sender to link with receiver or copy the receiver to answer to the sender.
VII. LITERATURE REVIEW

Deepa Panse (2014) proposed, Cloud computing is an internet-based computing, wherever regular resources and facilities such as presentations, storing and attendants are delivered through the Internet devices and computing. It integrates large open distributed system, virtualization, and internet services of delivery, dynamic provision of reconfigurable and on-demand operations. Growing and showing of consistent growth in the field of Cloud Computing is continuing. And also challenging task in cloud computing is caused by the outsourcing of infrastructure, sensitive information and critical requests, and its multi-tenancy nature the security and privacy issues.

For Cloud Computing security is emerging capacity for study and this paper describe the various categories of authentication and multi-factor consumer authentication [10].

Alexander D. Kent (2013), this paper discusses user validation which symbolize with the network activity within the graph. Dataset mechanism using the real enterprise connection, and also find out that non-restricted client, size and complexity, graph attributes in terms of system administration privileges. In accumulation, we find user behavior intuitive insights into network providing graphs. Sympathetic these modifications in level detail of lead to enhanced user behavior elusive detection and profiling of authentication documentation exploitation [11].

SeemaRao, Prof.K.J.Satoa (2013), proposed a verification technique of fingerprint system using perfect, debauched and effectual automatic presence system.

We present a scheme in the extraction of minutiae technique and quantitative approach fingerprint verification using extraction of minutiae technique, on fingerprint matching biometric technologies, learning showed that using a measurable approach by designing a questionnaire serves as the information gathering instrument. The Random sampling technique involved 6 employees based on stratified reasoning. The results, conversely represent was found suitable for the employee presence organization system of the fingerprint biometric identifier [12].

Ahmad Alamgir Khan (2013), in his research paper presents a fresh approach to contest the Phishing attacks. An outcome within reach is proposed where the client will take back the OTP (one time password) by short message service (SMS) or by alternate communication ID (email-id). After receipt of the OTP (one time password) the WS (web server) will compose an encrypted token for the client device for verification. The encrypted token will be used for acknowledgment, sometime, the client requests to access the website he/she have to apply for the new password. The OTP as the name implies will terminate after particular utilize. The OTP (one time password) and encrypted token are part of a smart technique to deal with this problem [13].

Pooja Kolte (2015) gave the idea of a client id and the secret word is one of the most effortless routes for verification. It is the most straightforward path, as well as practical and exceptionally effective. Today, we can see the secret key breaking and hacking in all around. At present we are utilizing the single server framework for this kind of secret key based confirmation. Traditional protocols for secret key based validation accept a single server which stores all the data (e.g., the password) important to confirm a client. In this paper, a fresh, well-organized two-server password-only based confirmation is planned where the customer can ascertain dissimilar cryptographic keys with the two servers. These two servers’ runs corresponding and collude with each other to validate the client [14].

VIII. PROPOSED WORK AND IMPLEMENTATION

First, we will start with a user registration form, using register button which is given on our website home page. If user is already registered it goes to the login form otherwise first it will register. In the registration form user will enter their details. After that Login form is open and the user will enter their email id which is given by the user at the time of registration. After user login, the next process has randomly generated query. Any one query generates randomly on the user web page, user will answer this query.
If the user doesn’t know the answer of this query than user has an option of “next question”. This option is available only 3 times. If the user gives the correct answer of the query which is asked by the server then the user has right to ask a query to the server, the user chooses any one query to server and server send the answer of that query on user email-id. If server answer isn’t correct and delay for answer than it means it is a fake web server. After this in the next process “check password” form is open in this page user can enter a password. If user submit the wrong password, then the user will be blocked. Only three times user can enter their password. Only three checks are available in this flowchart, first is the client check answer, next is the server check answer, and last the user password.

Fig. 8 flow diagram over authentication new technique
The shown results are:

1) Now, first home page contains the information of website user will interact with the home page. Show the fig 9. Three buttons are there; Home, Registration and Login button.

![Fig 9. Website home page](image)

In registration form, new users register here. After the registration successfully a “login form” will appear.

2) In the registration form, users will register and get their user id and password. Some basic information about the user will be entered and also answering of 25 questions are compulsory. Show in fig 10.

![Fig 10. Registration Form part (1)](image)

3) After registration form submission, another page will open that is user login page. In which user will enter the valid email-id. Show in fig 11.

![Fig 11. Login Form](image)

4) Next will be the Server Question Answer Form, now in this from the server will ask a one question to the user as query that is randomly generated Show in fig 12. If the user doesn't know an answer of this query, the user has an option of “next question” button. This option will available 3 times only. This page has a 3 minute time limit for a user query answer form.
5) If User enters the correct answer of the query, then the next step Client Question Answer Form will open, in concurrence to proposed algorithm user can ask any one query to server. And server sends the correct answer on the user email id which is registered by the user at the time of registration. Show in fig 13.

6) On the User Password Form page, a user can enter a password to login successfully. If the user enters three times a wrong password, then the user will be blocked. Show in fig 14.

7) This page represents that user has entered a wrong email id. If the user will repeat mistake 3 times, then this page will generate. Show in fig 15.

8) The following page will appear after the both Sides Successful Authentication. With the help of these steps user and server both authenticate to each other, now user can do whatever transaction he/she wants. Show in fig 16.
IX. CONCLUSION

In this work, we introduced a security validation procedure to defeat the issue of man in the middle attack in e-commerce. We likewise inspected of Phishing issue and the principal challenges in the outline of a security framework, we additionally examined the diverse confirmation strategy in our work we attempt to take care of a major issue in exchange security of MIMA with the assistance of our procedure first we confirm a server to a client then we validate client for the same server. In one way authentication, there is an only one side (client side) valid, but the other part (server) doesn’t validate the first one. Two ways authentications provide high security on both sides (client and server) authentication. In future work, we will apply the same on a cloud with the help of that we will provide a security on the cloud because cloud is a very vast structure and there is a need of security. And we will use key during the query transformation.

REFERENCES


