WEB SERVER AUTHENTICATION AND MONITORING SYSTEM

[1]PRAVIN KARANJULE, [2]SAYALI CHAVAN, [3]PANKAJ BAND,[4]ANKUSH PANDHARE, [4]SEEMA MANDLIK,

Professor, Department of Information Technology, MIT-Academy of Engineering, Savitribai Phule Pune University

Abstract—There are numerous loads on the web server due to tremendous use of Internet. There is an urgent need to be solved that monitoring the performance of web servers. This paper constructs authenticating and monitoring the performance of the web servers based on web services. This system provides authentication and monitoring performance based on the web services using java Technology. Here authentication is done by storing the password in two servers and monitoring is used to analyze the CPU usages, memory usages and bandwidth of valid hosts. The operations that can be performed by the system are authentication, subscription, scheduling and monitoring.

Index Terms—WSMR,WEB SERVICES, XML,SOAP, Elliptic curve cryptography, Password-authenticated key exchange.

I.INTRODUCTIOIN

Now a day's server management plays an important role as it enhances performance of the servers. The proposed system constructs an authenticated and monitored technology for server using web services.

For authentication purpose the concept of a user id and password is one of the easiest ways to authenticate.

Today, we can see password being cracked and hacked easily. Traditional protocols for password-based authentication assume a single server where it stores all the information (e.g., the password) necessary to authenticate a user. When an attacker obtains the information stored on the server, he can obtain all the passwords which were stored in the server via launching an off-line dictionary attack. To address this issue, number of schemes has been proposed in which a user's password information is stored among multiple servers and a new efficient two-server password based authentication is used.

Monitoring of web server has become urgent problem to be solved. So here the proposed system constructs a managing and monitored platform for server using technology of web services. According to the system, the utilization rate of CPU, Memory and Bandwidth can be monitored . The business logic of this system is promoted by technology of web services and java technology which provide data interface for the system.

II. LITERATURE SURVEY:

In 2010,LixinKe, Liang Zhou,Kaijun Wu[1] proposed a managing and monitored platform for servers based on the B/S architecture by using the technology of web services and flex.Thebusiness logic of this system is proposed by the technology of web services with javaEE architecture and the web page presentation of the system is supported by flex technology.Zhen Liu, Nicolas Niclausse, [2]proposed a paper in 2001, they proposed a traffic model at session level which describes when users arrive and how they browse the server,they developed a web

server benchmark“WAGON” (web traffic generator and benchmark) and validated the traffic model by comparing various characteristics of synthetic traffic generated by WAGON against measurements.DiegoZuquimGuimarães Garcia,[3] proposed a fault tolerant web service a web services have been pointed as a suitable technology for the development and execution of distributed applications.The web service architecture still lacks facilities to support fault tolerance.The goal is to propose a fault tolerant web service architecture.The architecture of this system provides service mediation and monitoring.The purpose of this paper is the use of web service standards to include fault tolerance in the Web service architecture.AnithaKumari, Dr.SudhaSadasivam, [4] proposed in 2013 a PAKE (password based authentication and key exchange) it is designed for single server environment where each user shares a password with server.Two server protocol split the password into two long shares and stores in different servers such that if one server attacked will not provide the useful information about the password.Vignesh Kumar Kanglulakshmi [5], proposed a system in 2012 wherein user’s password information is shared among multiple servers and these servers cooperate in a threshold manner user wants to authenticate.They recommend using two servers namely front end server and back end server the password is split and stores in these two servers and even if one server is compromised then the other server will be having the password saved.Xun Yi, San Ling [6],proposed a system in 2013 where a client and a server who share a password authenticate each other and meanwhile establish a cryptographic key by exchange of messages.Here in this system all the passwords necessary to authenticate clients are stored in a single server.If the server is compromised then the password stored in the server are all disclosed.In this paper, they consider a scenario where two servers cooperate to authenticate a Client and if one server compromised, then attacker still cannot pretend to be the client with the information from the compromised Server.

III. PROPOSED SYSTEM

Public key technique are prone to make password system secure against offline dictionary attacks whereas improvement of public under the PKI.

(e.g., public key encryption and digital signature schemes) is not essential. Three are two separate approaches to the development of secure password system one is combine use of a password and public key crypto-system under the PKI and other is a password only approach. In this system the user of public keys is involved in the development and maintenance of PKI for public key certification and adds to users the burden of checking key validity. To eliminate this drawback, password authentication key exchange (PAKE) has been extensively studied.The PAKE protocols do not involve any public key crypto system under the PKI and they are much more attractive for real world application.Any use of public key crypto system under PKI in a password authentication system should be avoided. The benefits of the use of password would be counteracted to great extent.Most of the existing password system designed over a single server, where each user shares a password verification data (PVD) with single Authentication server. This system is essentially intended to defeat offline dictionary attacks by outside attackers and assumes that server is completely trusted in protecting the user password database.

In case of existing system main focus is on monitoring,itdosenot use the web server technology so it creates problem for cross platform communication.There is no provision for automatic scheduling.Including these there are other limitations like high complexity and slow reaction.

In case of proposed system, the system describes a cross-platform management and monitoring system for server based on B/S mode by using the web services on J2EE technology, which has better effect on cross platform application, immediate response,

user interaction, maintenance and deployment. This system provides automatic scheduling and it can monitor multiple servers.

Advantages:

- Automatic scheduling
- Multi-server monitoring
- Web services

IV.ARCHITECTURE

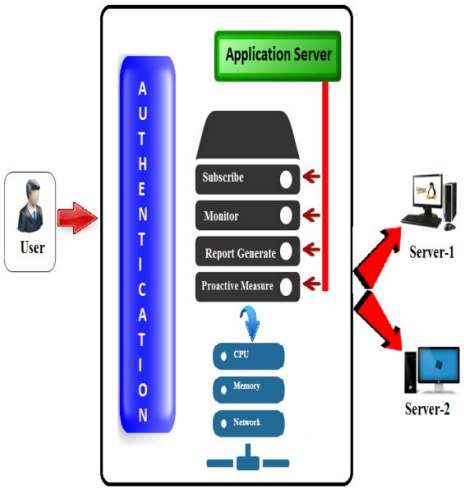

Figure1. Architecture OfWeb Server Authentication And MonitoringSystem

The above figure is a architecture of web server authentication and monitoring consists of two phases that is first is the authentication phase and then the monitoring phase.

Authentication Phase:

In authentication phase, it provides a secure authentication where the password is splited and stored in two servers therefore providing security even if one server is compromised by the attacker. Diffie Hellman key exchange protocol is used when the key is entered by the user for mutual authentication. Encryption of password is done with the help of Elliptic curve cryptography.

Monitoring Phase:

The monitoring phase consists of following functions which are performed are:

1] Subscription:

Firstly client require to register.If already subscribed then login system administrator has to enter IP address to start monitoring process and then subscribed user has to enter his requirement.

2] Scheduling:Manual or automatic scheduling as per user requirement.

3] Monitoring:Checking performance parameters like CPU usage,network,memory.

4] Proactivemeasures:Processes are arranged in priority and dependency.Accordingtopriority terminate process.

V. ALGOLITHM

1.Diffie-Hellman Key Exchange Algorithm

Input: $q$is prime number and $g<q$.

1. User A key generation

1. Select private key m.

2. Calculate KA =g^m mod q

2. User B key generation

1. Select private key n.

2. Calculate KB = g^n mod q

3. Calculation of Secret key by user A

$K_1 = (B)^m$ mod q

4. Calculation of Secret key by user A

$K_2 = (A)^n$ mod q

5. Obviously$K_1=K_2$.So this will be shared secret key among A and B.

Output: K1, K2.

2. EllipticCurveAlgorithmKey Generation:

Input: Elliptic curve domain parameters (p, E, P, n).

1. Select d belongs to R in range [1, n−1].
2. Compute Q = d*P.
3. Return (Q, d).

Output: Public key Q and private key d.

A. Encryption Algorithm:

Input: Elliptic curve domain parameters (p, E, P, n)
, Public key Q, plaintext m.

1. Represent the message 'm' as a point M in E (Fp).
2. Select 'k' belongs to R in range [1, n−1].
3. Compute C1 = k*P.
4. Compute C2 = M + (k*Q).
5. Return (C1, C2).

Output: Cipher text (C1, C2).

B. Decryption Algorithm:

Input: Domain parameters (p, E, P, n), private key d,
cipher text (C1, C2).

1. Compute M = C2−dC1, and extract m.
2. Return (m).

Output: Plaintext m.

VI. CONCLUSION

The web server authentication and monitoring is based on web service that provide a way to authenticate and monitor the web servers..The proposed system will provide more security as compared to existing system by two server authentication and monitoring of the web servers will be done on different parameters and it will be done automatically reducing the manual burden and mainly providing the cross platform monitoring.

VII.REFERENCES

[1] LixinKe, Liang Zhou, Kaijun Wu," The Construction of Servers Monitoring Platform Based on Web Services",IEEE,2010.

[2] Zhen Liu□, Nicolas Niclausse, César Jalpa-Villanueva1," Traffic model and performance evaluation of Web servers",IEEE 2011.

[3] Diego ZuquimGuimarães Garcia, Maria Beatriz Felgar de Toledo," A Fault Tolerant Web Service Architecture",IEEE,2010.

[4] AnamikaChouksey, YogadharPandey," An Efficient password based Two-Server Authentication and Pre-shared Key Exchange

System using Smart Cards",IJCSIT 2013.

[5] Vigneshkumar k, 2angulakshmi t, 3manivannan d, 4seethalakshmi r, 5swaminathan," password based two server authenticationSystem",issn 2012.

[6] AnithaKumari K1, Dr.SudhaSadasivam G2, Madhumitha R3,"A Review: PAKE Security for Distributed Environment",ISSN 2013.

[7] Xun Yi, San Ling, and Huaxiong Wang," Efficient Two-Server Password-OnlyAuthenticated Key Exchange",IEEE 2013.

[8] KuldeepBhardwaj and Sanjay Chaudhary," Implementation of Elliptic Curve Cryptography in 'C'",ISSN 2012.