Multifactor Authentication For Secure Banking

N.Bhavani[1], B.Praveen[2], N.Srinivasan[3], S.Srithar[4]
[1, 2, 3, 4]Dept of Information Technology
[1, 2, 3, 4,]Saranathan College of Engineering, Tiruchirapalli-620012, TamilNadu, India

Abstract- *Authenticated Key Exchange (AKE) protocol permits a user and a server to authenticate each other for the first time. It generates a session key for the successive communications without any authentication. In this work, a novel Multi Factor AKE protocol is proposed in banking application to overcome problems present in current banking system. Multifactor authentication combines two or more independent credentials. First credential has user defined user name and password verification process. This protocol supports the key stroke based password authentication process. The average time to enter a password will be defined. The user has to type the password within the allocated time, failing which he / she have to enter it again. Then second factor uses the face recognition process. The goal of MFA (Multi Factor Authentication) is to create a layered defence and make it more difficult for an unauthorized person to access a banking application. Third factor is to generate the session key for secured communication. Session key will be share to the corresponding receiver. Receiver should also verify using Multi Factor Authentication system and get session key for communication verification. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.*

Keywords- Security, Password Authentication, Session Key

I. INTRODUCTION

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of service and network-accessible resources. Networksecurity involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It secures the network, as well as protecting and overseeing operations being done.

The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password— this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g., a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wire shark traffic and may be logged for audit purposes and for later high-level analysis. Newer systems combining unsupervised machine learning with full network traffic analysis can detect active network attackers from malicious insiders or targeted external attackers that have compromised a user machine or account. Communication between two hosts using a network may be encrypted to maintain privacy.

II. LITERATURE SURVEY

1.Three Party Authentication Scheme for RFID Systems in IOT

Focuses on improving the security of RFID systems in IoT. RFID technology is an automatic data capturing technology which uses radio frequency to identify objects. Previously its application range was limited to management systems to identify the product, object or person and some payment systems.However, with the emergence of the smart world and IoT, the application areas of RFID technology have been spread widely. Now it is considered as one of the strong candidates for automating environment. With the increase in the use of RFID technology, reliability and security of the communication have become one of hot research topics. There have been many authentication protocols proposed for the secure communication in RFID systems. However, most of the approaches were presented when RFID tags were purely used in supply chain management as replacement of the bar-code.

2.An Effective and Robust Secure Remote User Authenticated Key Agreement Scheme using Smart Cards in Wireless Communication Systems

Presents a more secure and robust remote user authenticated key agreement scheme in order to remedy the security flaws. Through the formal security analysis using the widely-accepted Burrows– Abadi–Needham logic (BAN logic), this scheme provides secure mutual authentication. Furthermore, the formal and informal security analysis show that this scheme is secure against various known attacks including the offline password guessing attack when smart card of a user is lost/stolen, and this scheme also provides SK-security, user anonymity and avoids the time- synchronization problem. This scheme is simulated for the formal security verification using the widely-accepted and widely-used Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. Thus, understanding the security failures of authentication schemes is a key for both patching to the existing schemes and designing the future schemes.

3.A secure single sign-on mechanism for distributed computer networks

Proposed a secure single sign-on mechanism that is efficient, secure, and suitable for mobile devices in distributed computer networks. User identification is an important access control mechanism for client–server networking architectures. The concept of single sign-on can allow legal users to use the unitary token to access different service providers in distributed computer networks. Recently, some user identification schemes have been proposed for distributed computer networks. Unfortunately, most existing schemes cannot preserve user anonymity when possible attacks occur. Also, the additional time- synchronized mechanisms they use may cause extensive overhead costs. To overcome these drawbacks, this paper is designed. With the development of distributed computer networks, it is easy for user terminals to share information and computing power with hosts. The distributed locations of service providers make it efficient and convenient for subscribers to access the resthisces. In general solutions, users must register with each service provider and keep different identity/password pairs for accessing each service provider. However, when users have to keep so much secret information, security problems can occur and increase the overhead for the networks. In this paper, we propose a secure single sign-on mechanism to allow mobile users to use the unitary token to access service providers. In a real- life application, the mobile user can use the mobile device, e.g., a cell phone, with the unitary token to access multi services, such as download music, receive/reply electronic mails, order goods, or process online payment etc., from different service providers in distributed computer networks. This scheme is based on one-way hash functions and random nonces to solve the weaknesses described above and to decrease the overhead of the system.

III. EXISTING SYSTEM

Authenticated Key Exchange (AKE) protocol allows a person and a server to authenticate every different and generate a session key for the subsequent communications. With the speedy improvement of low-power and especially efficient networks like pervasive and mobile computing community in recent years, many green AKE protocols have been proposed to acquire person privateness and authentication in the communications. Besides at ease consultation key establishment, the ones AKE protocols provide a few other beneficial capabilities like -element consumer authentication and mutual authentication. Existing work take DDH as the fundamental assumption, because it is well-known for achieving key exchange with just two group elements and two group operations, which means low communication and computation complexity. But it cannot resist man-in-the-middle attack, so our work is to put the authentications for all three factors with the DDH like key exchange together. Two different generators for a same group are used here to achieve this purpose. Here the basic idea is that only one knows all three factors can derive the correct part information for DDH-like key exchange, else he cannot guess the session key with just one part information. In addition, the group additive operation on the shoulder has homomorphic property, which makes the authentication for three factors can be finished in parallel and the number of factors can be adjusted as needed.

IV. PROPOSED SYSTEM

A novel Multi Factor AKE protocol is proposed to overcome all the weaknesses in the existing system. This protocol supports keystroke authentication and bio metric verification process. The users should register their banking details to make transaction through this application. The average time to enter a password will be defined. The user has to type the password within the allocated time, failing which he / she have to enter it again. This security model of AKE supports user anonymity and resist lost card attack. Then they could be capture their face image in real time then extract the features form face image and store that features with label of the customer details. Elliptical Curve Cryptography algorithm is used for encryption and decryption of the session key. The computational cost and the bandwidth cost for this proposed model are low, which makes it to use in pervasive computing applications and mobile communications. The proposed AKE model is much secured when compared to the existing protocols.

V. SYSTEM ARCHITECTURE

Software architecture involves the high level structure of software system abstraction, by using decomposition and composition, with architectural style and quality attributes. A software architecture design must conform to the major functionality and performance requirements of the system, as well as satisfy the non-functional requirements such as reliability, scalability, portability, and availability.

Software architecture must describe its group of components, their connections, interactions among them and deployment configuration of all components.

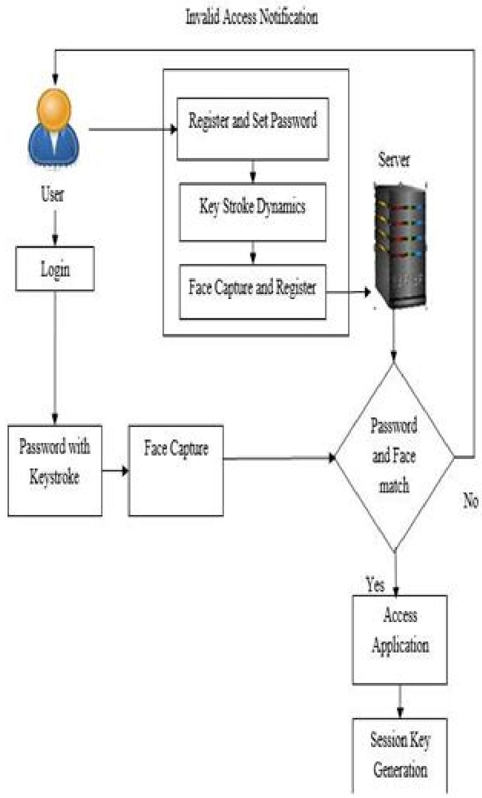

Fig 1. System architecture

Description:

A novel Multi Factor AKE protocol is proposed to overcome all the weaknesses in the existing system. This protocol supports keystroke authentication and bio metric verification process. The users should register their banking details to make transaction through this application. The average time to enter a password will be defined. The user has to type the password within the allocated time, failing which he / she have to enter it again. This security model of AKE supports user anonymity and resist lost card attack. Then they could be capture their face image in real time then extract the features form face image and store that features with label of the customer details. Elliptical Curve Cryptography algorithm is used for encryption and decryption of the session key.

The computational cost and the bandwidth cost for this proposed model are low, which makes it to use in pervasive computing applications and mobile communications. The proposed AKE model is much secured when compared to the existing protocols.

VI. MODULES

A. User Enrollment

Online transaction is thus changing the way people shop and how retailers operate. However, this technology and digital convergence has also attracted the threat of cyber-attacks and made banks and financial institutions more vulnerable to fraud. To overcome, these attacks, we can design the interface for online transactions in banking system. In this module, admin and user interface created. In this application User has to register the appropriate details in the bank server database for using the online banking template. These details include user name, address, email id, contact number, primary password and keystroke value. Also capture the face image and register for bio metric verification. These details are stored in the first server database.

B. Password Authentication

Anonymous access is the most common web site access control method, which allows anyone to visit the public areas of a website while preventing unauthorized users from gaining access to a critical features and private information of web servers. The user verification phase analyzes the user name, password, keystroke value to the bank server. During password verification, key stroke time for password will be calculated and matched with database. User should enter the password with the specified time, otherwise they will not allow to access application.

C. Face Biometric Verification

The Face Recognition is the study of physical or behavioural characteristics of human being used for the identification of person. These Face Recognition features can be used to make net-banking systems more secure for authentication purpose in banking based account security systems. In this module, we can implement features based method to detect the facial parts such as nose, lips, eyes, cheeks using iterative closest point algorithm. In this module we use, for performing ICP that is Iterative Closest Point algorithm is used as a set of features selected based on the tolerance level of spatial deviation. This allows a rapid convergence of the algorithm which processes only these points and cancels points which presents spatial deviation value superior to the tolerance value. In contrast, correspondence concerns all intersecting points.

D. Session Key Agreement

In proposed banking facility, when user making transaction session key will generated automatically. The session key will ensure the communication between sender and receiver. Admin would need to register with the institution for the provider, and set up a password and different credentials for user verification. The session key generation process fully based on the asymmetric algorithm. Public-key cryptography is based on the intractability of distinctive mathematical issues. Early public-key methods are cozy assuming that it is tricky to element a massive integer composed of two or extra giant top causes. For elliptic-curve-headquartered protocols, it's assumed that finding the discrete logarithm of a random elliptic curve detail with respect to a publicly recognized base factor is infeasible: this is the "elliptic curve discrete logarithm trouble" (ECDLP).The security of elliptic curve cryptography is dependent upon the potential to compute a factor multiplication and the incapability to compute the multiplicand given the customary and product points. The size of the elliptic curve determines the problem of the concern. The primary improvement promised through elliptic curve cryptography is a smaller key dimension, lowering storage and transmission requisites.

E. Secured Communication

Sender encrypt the given data and Receiver should complete the verification criteria then access banking application. In ATM application, user can perform transaction, withdrawal, balance enquiry and mini statement details. After the verification process login to the account, the server can be provided the session key to the login user. Receiver should enter the session key for authenticate the process and view the transaction process.

VII. CONCLUSION

A secure Multi – Factor AKE scheme was proposed to provide security against various attacks including de-synchronization attack, lost-smart-card attack and password guessing attack, and supports several desirable properties including perfect forward secrecy, anonymity or untraceability, adaptively password change, no centralized password storage and no long-term public key. Furthermore, this protocol maintains high efficiency in terms of storage requirement, communication cost as well as computational complexity. The proposed scheme is provably secure in this extended security model of AKE.

VIII. FUTURE WORK

In future, various cryptographic algorithms are implementing to improve the performance of multi factor authentication and increase the integrity and confidentiality of shared information. Also focus on developing mobile application for secure communication with multi factor authentication scheme.

REFERENCES

[1] C. Chang and C. Lee, "A secure single sign-on mechanism for distributed computer networks," IEEE Trans. Ind. Electron., vol. 59, no. 1, pp. 629-637, Jan. 2012.

[2] C. Chang, H. Le, C. Lee, and C. Chang, "A robust and efficient smart card oriented remote user authentication protocol," Intelligent Information Hiding and Multimedia Signal Processing(IIHMSP), 2011 Seventh International Conference on, pp.252 - 255, 2011.

[3] M. Hwang, and L. Li,"A new remote user authentication scheme using smart cards," IEEE Trans. Consume. Electron., 2000, 46(1):28-30.

[4] Y. Huang, W. Lin, and H. Li,(2012) "Efficient Implementation of RFID Mutual Authentication Protocol," IEEE Trans. Ind. Electron., vol. 59, no. 12, pp. 4784 - 4791, 2012.

[5] Jue-Sam Chou, Yalin Chen, Cheng-Lun Wu, Chi- Fong Linv, “An efficient RFID mutual authentication scheme based on ECC”, IACR Cryptology, 2011.

[6] Jongho Moon, Donghoon Lee, Jaewook Jung and Dongho Won, “Improvement of Efficient and Secure Smart Card Based Password Authentication Scheme”, International This work of Network Security, Vol.19, No.6, PP.1053-1061, Nov. 2017.

[7] Soothar, Virlla Devi. Three Party Authentication Scheme for RFID Systems in IoT. Diss.2017.

[8] Vanga Odelu, Ashok Kumar Das and Adrijit Goswami,“An Effective and Robust Secure Remote User Authenticated Key agreement Scheme Using Smart Cards in Wireless Communication Systems” , Wireless Personal Communications, October 2015, Volume 84, Issue 4, pp 2571–2598.