INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

Multi factor AKE protocol and key stroke authentication for secured communication

S. Kanimozhi
kanimozhi6695@gmail.com
Anna University BIT-Campus, Tiruchirappalli, Tamil Nadu

S. Jayanthi
dharsh02@yahoo.com
Anna University BIT-Campus, Tiruchirappalli, Tamil Nadu

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. Many AKE protocols had been proposed to obtain person privateness and authentication for the duration of conversation. Other than secured consultation key established order, these AKE protocols offer a few other useful capability like two-thing user authentication and mutual authentication. But they have got few weaknesses along with vulnerability in opposition to loss of smart card, offline dictionary assault, de-synchronization attack, person anonymity or untraceability. Also, AKE scheme the usage of public key conversation doesn't suite nicely for lightweight computational gadgets. In this work, a novel Multi-Factor AKE protocol is proposed to overcome all the above-mentioned weaknesses. This protocol supports revoked smart card transactions. The password that is available on the USB device will be overwritten once the user used it. Passwords can be updated without centralized storage. 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 has to enter it again. This security model of AKE supports user anonymity and resist a lost card attack. 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 useful in pervasive computing applications and mobile communications. The proposed AKE model is much secured when compared to the existing protocols.

Keywords— *Multi-factor authentication, AKE (Authenticated Key Exchange) Protocol, Key stroke authentication, Session key generation, ECC Encryption*

1. INTRODUCTION

1.1 Network security basics

Network security includes the guidelines and practices that are adapted to prevent and display unauthorized access, misuse, modification, or denial of a computer network and community-accessible assets. Network security involves the authorization process of access to data in a network, which is controlled and maintained by the network administrator. Users are assigned a unique ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a maximum type of computer networks, both public and private, which can be utilized in normal jobs; accomplishing transactions and communications among corporations, authorities companies, and individuals. Networks can be private, such as within a company or any other organization, and others which might be open to public access. Works of network security involved in organizations, enterprises, and other types of institutions. It does as its title explains: It is used to secure the network, as well as protecting and overseeing operations being done. The most commonly used and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

1.2 Network Security

Network security first initializes with authenticating, commonly with a username and a password. Since this necessitates just one detail authenticating the user name that is, the password, this is sometimes termed one-factor authentication. In two-factor authentication, something the person 'has' is likewise used (e.g., a protection token or 'dongle', an ATM card, or a mobile smartphone); and additionally with 3-factor authentication, the user 'is' extensively utilized biometric like (e.g., a fingerprint or retinal scan).

Honeypots, basically decoy network-to-be had sources, can be deployed in a network as surveillance and early-caution system because the honeypots aren't usually accessed for legitimate functions. Techniques utilized by the attackers that try to compromise those decoy sources are studied throughout and after an attack to hold an eye on new exploitation strategies. Such analysis can be used to similarly tighten safety of the actual network being included by the honeypot. A honeypot also can direct an attacker's interest away from valid servers. A honeypot encourages attackers to spend their time and electricity on the decoy server even as distracting their interest from the data at the real server. Similar to a honeypot, a

honeynet is one type of a network set up with intentional vulnerabilities. Its cause is likewise to invite assaults in order that the attacker's methods may be studied and that facts can be used to growth network security. A honeynet usually consists of one or more honeypots.

1.3 Security Management

Security management for networks is different based on different situations. Small businesses like a home or small workplace may additionally best require basic protection while big groups or businesses may also require high-upkeep and advanced software and hardware to prevent malicious assaults from hacking and spamming.

1.4 Types of Attacks

Networks are issue to attacks from malicious sources. Attacks can be from classes: "Passive" at the same time as a community intruder intercepts data at some point of sending thru the community, and "Active" in which an interloper initiates commands to disrupt the community's normal operation or to behavior reconnaissance and lateral movement to locate and advantage access to property to be had via the network.

1.5 Access manipulate

Not each consumer need to have access to your network. To preserve our capability attackers, you need to apprehend every consumer and every tool. Then you could put into effect your safety rules. You can block noncompliant endpoint devices or provide the most effective limited get entry to. This process is community get entry to control (NAC).

1.6 Antivirus and antimalware software program

Malicious software is called for Malware that has viruses, worms, Trojans, ransomware, and adware. Sometimes malware will infect a network but lie dormant for days or maybe weeks. The quality antimalware packages no longer handiest scan for malware upon entry, but also continuously music documents afterward to discover anomalies, do away with malware, and attach damage.

1.7 Application protection

Any software you operate to run your business wishes to be covered, whether or not your IT personnel builds it or whether or not you buy it. Unfortunately, any utility can also comprise holes, or vulnerabilities, the ones attackers can use to infiltrate your network. Application security encompasses the hardware, software, and techniques you use to shut the one's holes.

1.8 Behavioral analytics

To stumble on unusual community behavior, you should recognize what everyday conduct looks like. Behavioral analytics tools automatically parent activities that deviate from the norm. Your security crew can then better pick out indicators of compromise that pose a capability problem and speedy remediate threats.

1.9 Email protection

Email gateways are the number one threat vector for a safety breach. Attackers use personal facts and social engineering techniques to build sophisticated phishing campaigns to mislead recipients and send them to web sites serving up malware. An email protection utility blocks incoming attacks and controls outbound messages to prevent the loss of sensitive facts.

1.10 Firewalls

Firewalls positioned up a barrier between your trusted inner community and untrusted outdoor networks, which includes the Internet. They use a hard and fast of defined regulations to permit or block traffic. A firewall can be hardware, software program, or both. Cisco gives unified hazard. control (UTM) devices and danger-targeted next-generation firewalls.

1.11 Intrusion prevention structures

An intrusion prevention machine (IPS) scans network site visitors to actively block assaults. Cisco Next-Generation IPS (NGIPS) appliances try this by way of correlating big amounts of world risk intelligence to no longer only block malicious interest but additionally tune the progression of suspect files and malware throughout the network to prevent the unfold of outbreaks and reinjection.

1.12 Mobile tool safety

Cybercriminals are increasingly more targeting cell gadgets and apps. Within the next 3 years, 90 percentage of IT companies may also help corporate packages on personal cellular gadgets. Of path, you need to manipulate which devices can get admission to your community. You will even need to configure their connections to preserve network traffic non-public.

1.13 Network segmentation

Software-defined segmentation puts network visitors into one of a kind classifications and makes imposing safety rules easier. Ideally, the classifications are based on endpoint identification, not mere IP addresses. You can assign get right of entry to rights primarily based on function, area, and extra so that the proper stage of getting right of entry to is given to the proper human beings and suspicious gadgets are contained and remediated.

1.14 Security information and event management

SIEM products pull collectively the information that your safety body of workers needs to pick out and reply to threats. These products are available in numerous paperwork, which includes physical and virtual home equipment and server software program.

1.15 Web security

A web protection solution will manipulate your staff's internet use, block web-based totally threats, and deny get admission to malicious web sites. It will shield your web gateway on the website online or inside the cloud. It also refers to the companion way you take to defend your own internet site.

1.16 Wireless safety

Wireless networks are not as at ease as stressed ones. Without stringent security measures, putting in a wi-fi LAN may be like setting Ethernet ports anywhere, along with the car parking zone. To save you an exploit from taking maintain, you need merchandise specifically designed to protect a Wi-Fi community.

2. RELATED WORK

B. Wang, et.al, [1] Proposed a brand new protocol with two authentic methods, which might be the label sharing approach to shield customer and the detachable principal database method to beautify gadget mobility is proposed on this paper. The security properties of the brand new scheme are proven by way of the usage of Colored Petri Net (CPN) and algebra proofs. The significance of radio frequency identity (RFID) protection is increasing explosively, main to a studies fashion. The modern maximum extreme RFID protection issues are privateness and authentication protection. The renewable identity (ID) method with a vital database is the modern dominating method to achieve user privacy and authentication

safety. Although, the approach will motive greater problems that renewable ID will growth RFID tag fee and will allow denial of service (DoS) attacks while the relevant database will lessen system mobility. To solve the catch 22 situation, this paper is supplied. In this paper, as this major contributions, a comfortable and strong authentication scheme (USI) for the RFID device, RFID reader unbiased approach and the tag label sharing method are proposed. The system's safety capability to save you tag tracing attacks and DoS attacks with the support of mobility has been formally proven by means of Colored Petri Net (CPN) models.

C. Chang, et.al, [2] Proposed an ease unmarried sign-on mechanism that is efficient, relaxed, and appropriate for cellular gadgets in dispensed laptop networks. User identity is an essential get admission to manage mechanism for the client-server networking architectures. The concept of unmarried sign-on can allow felony users to use the unitary token to get right of entry to distinctive provider vendors in dispensed computer networks. Recently, some consumer identification schemes were proposed for allotted pc networks. Unfortunately, maximum current schemes can't preserve user anonymity whilst possible assaults arise. Also, the extra time-synchronized mechanisms they use can also cause sizeable overhead costs. To conquer those drawbacks, this paper is designed. With the improvement of disbursed computer networks, it is easy for consumer terminals to share facts and computing strength with hosts. The disbursed locations of carrier companies make it efficient and handy for subscribers to get entry to the resources. In standard answers, customers should sign in with each provider company and preserve extraordinary identity/password pairs for accessing each service issuer. However, when users must keep a lot of secret statistics, security problems can arise and growth the overhead for the networks. In this paper, we suggest a secure unmarried sign-on mechanism to permit cell customers to apply the unitary token to get admission to carrier companies. This scheme is based on one-way hash features and random nonces to resolve the weaknesses defined above and to lower the overhead of the system.

C. Chang, et.al, [3] Analyzes security flaws and then proposes a protocol that overcomes all of the weaknesses of the aforementioned protocol. Authentication and key agreement protocols are the basis for the security of distributed packages. In proposed authenticated key settlement protocols. Features consumer's anonymity. However, we determined that the second one scheme is prone to replay assault, masquerade assault, and rancid-line password attack. Owing to statistics technology speedy development, lots of disbursed applications, inclusive of e-commerce, banks, content distribution systems, airline reservation systems are broadly advanced and deployed over the Internet. This ends in the security worries in their information confidentiality and the privacy of the structures' customers. Therefore, it requires a strong and efficient authenticated key settlement protocol to help those packages. In 1981, Lamport delivered the primary password-based remote authentication protocol. After that, Hwang, Lo and Yeh proposed static ID-primarily based far-flung authentication schemes that send the users' ID in plaintext to the server over an insecure channel. Their strategies permit malicious adversaries to reveal and hint users. Subsequently, Das first proposed dynamic ID primarily based authentication protocol. However, the scheme changed into proved to be prone to password guessing assault by way of Liao. Since then, there have been many attempts to resolve password guessing assault hassle. Unfortunately, those schemes couldn't attain mutual authentication.

Jongho Moon, et.al, [4] Proposed a new authentication and key agreement scheme the use of clever card. In addition, we demonstrate that the proposed authentication scheme has sturdy resistance to the diverse attacks. Finally, we examine the overall performance and capability of the proposed scheme with different related schemes. Since Lamport proposed the primary password-primarily based authentication scheme over insecure communique in 1981, password-based total authentication schemes have been drastically investigated. However, the first-rate problem of password-based far-flung person authentication scheme is that a server ought to hold a password desk for verifying the legitimacy of a far-flung user. Therefore, the server calls for extra memory space for storing the password table for verifying consumer identification. Furthermore, the password is typically simple and may be without difficulty damaged or forgotten. For this cause, many researchers have proposed a new far-flung person authentication scheme by the usage of biological characteristics of individuals consisting of fingerprint, iris and so forth. The fundamental property of using biometric is its strong point. In the view of the fact that many far-flung user authentication schemes using organic characteristics were proposed.

M. Hwang, et.al, [5] proposed a new faraway consumer authentication scheme the usage of smart playing cards. This scheme is based totally on ElGamal's public key cryptosystem. This scheme does no longer require a gadget to keep a password table for verifying the legitimacy of the login users. This scheme can resist message replaying attack. This scheme is split into three phases. 1) Registration phase 2) Login segment and three) Authentication section. The simulation consequences really suggest that the proposed scheme is safe. Thus, this scheme offers excessive protection along with greater capability functions in comparison to Li et al.'s scheme and Islam's scheme. As a result, this scheme could be very appropriate for sensible packages. Authentication protocol in Wi-Fi communication systems is essential to defend the touchy facts towards a malicious adversary with the aid of supplying a ramification of services, which include person credentials' privacy, session key safety (we name it as SK protection), mutual authentication, and user revocation facility when a consumer's credentials are found out.

3. PROPOSED SYSTEM

A novel Multi-Factor AKE protocol is proposed to overcome all the weaknesses in the existing system. This protocol supports revoked smart card transactions. The password that is available on the USB device will be overwritten once the user used it. Passwords can be updated without centralized storage. 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 has to enter it again. This security model of AKE supports user anonymity and resist a lost card attack. 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 useful in pervasive computing applications and mobile communications. The proposed AKE model is much secured when compared to the existing protocols.

3.1 Methodology for the proposed work

Elliptical Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a way to public-key cryptography set up on the algebraic constitution of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (centered on undeniable Galois

fields) to provide similar security. Elliptic curves are applicable for the key contract, digital signatures, pseudo-random generators, and different duties. Indirectly, they may be able to be used for encryption by using combining the important thing agreement with a symmetric encryption scheme. They are also used in a couple of integer factorization algorithms based on elliptic curves that have purposes in cryptography, similar to Lenstra elliptic-curve factorization.

Elliptical curve cryptography (ECC) is a type of public key encryption approach. In Elliptic curve perceptions that can be created fast, smaller, and more effective cryptographic keys. ECC generates keys by means of the houses of the elliptic curve equation instead of the typical approach of new release because of the product of very tremendous prime numbers. The technological know-how can be utilized together with most public key encryption ways, comparable to RSA, and Diffie-Hellman. In accordance to some researchers, ECC can yield a stage of safety with a 164-bit key that different systems require a 1,024-bit key to achieve. Seeing that ECC helps to establish similar protection with lesser computing power and battery usage, it is becoming greatly used for cellular purposes. ECC was once developed through Certicom, a mobile e-business protection supplier, and was once not too long ago licensed by means of Hifn, a brand of built-in circuitry (IC) and network security merchandise. RSA has been setting up its own variation of ECC.

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. The security of elliptic curve cryptography is dependent upon the capability to compute an aspect multiplication and the lack of ability 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.

3.2 Steps in ECC algorithm

Encryption

(a) Define a Curve.
(b) Generate public-private Key pair the use of that curve, for each sender and receiver.
(c) Create a shared secret key from the key pair.
(d) From that shared secret key, create an encryption key.
(e) Using that encryption key and asymmetric encryption set of rules, encrypt the facts to send.

Decryption

The sender will both share the curve with the receiver or sender and receiver will have equal use for the equal curve form. Also, the sender will send its public key to the receiver.

(a) Generate public personal Key pair using the same curve for that curve for the receiver.
(b) Regenerate a shared secret key utilizing the private key of the receiver and the public key of the sender.
(c) From that shared secret key, create an encryption key.
(d) Utilizing that encryption key and symmetric encryption algorithm, decrypt the information.

3.3 General procedure of ECC

- Sender and Receiver conform to a few publicly-recognized information
- The elliptic curve equation
- Values of *a* and *b*
- Prime, *p*
- The elliptic group values are computed from the elliptic curve equation
- Basepoint B is taken from the elliptic group
- The similar generator used in current cryptosystems
- Each consumer generates its public/non-public key pair

Private Key = an integer, x, selected from the c language [1, p-1]
Public Key = product, Q, of personal key and base point (Q = x*B)

4. SYSTEM FRAMEWORK

4.1 User Enrollment

User has to register the appropriate details in the bank server database for using the online banking template. These details include a user name, address, email id, contact number, primary password, keystroke value, etc... These details are stored in the first server database.

4.2 Anonymous User 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 critical features and private information of web servers. The user verification phase analyzes the user name, password, keystroke value to the bank server. The second stage verifies the USB device value in the second password. Both verifications give permission to the user to access the online bank template and then changes the second password value. The second server overwrites the value into the USB device and informs the changed value to the account holder through email or SMS.

4.3 Session Key Agreement

After the verification process login to the account, the server can be provided the session key to the login user. Once the user is logged into the bank template, an alert message will be generated and send to the user. The session key generation process fully based on the ECC (asymmetric) algorithm. This agreement establishes secured communication between the user and the bank server. Using ECC, the session key is generated for the transaction. This session key is used to complete the transaction. ECC calls for smaller keys in comparison to other non-ECC cryptography to provide equivalent protection. ECC is able to provide the same cryptographic strength in security as an RSA-based system with much smaller key sizes. For example, In ECC a 256-bit key is equivalent to RSA 3072 bit keys (which are 50% longer than the 2048 bit keys commonly used today). The small key sizes make ECC very effective for devices with restricted storage or processing strength, which are turning into increasingly common in the secured conversation procedure. In terms of more traditional security purpose based on ECC algorithm for the smaller key sizes and stronger security.

4.4 Online Banking Template

Online banking, also called internet banking, e-banking or digital banking, is an electronic payment service that enables customers of a financial institution or different economic institution to conduct more than a few economic transactions via the economic organization's website. The online banking system will normally connect to or be part of the core banking system operated by using a bank and is in comparison to department banking which became the conventional way clients accessed banking offerings.

To get access to a monetary institution's online banking facility, a client with net access would need to register with the institution for the provider, and set up a password and different credentials for client verification. The credentials for online banking are typically no longer similar to for mobile banking. Financial establishments now routinely allocate clients numbers, whether or not customers have indicated an aim to get access to their online banking facility. Customer numbers are normally now not similar to account numbers, because a number of consumer accounts may be related to the account.

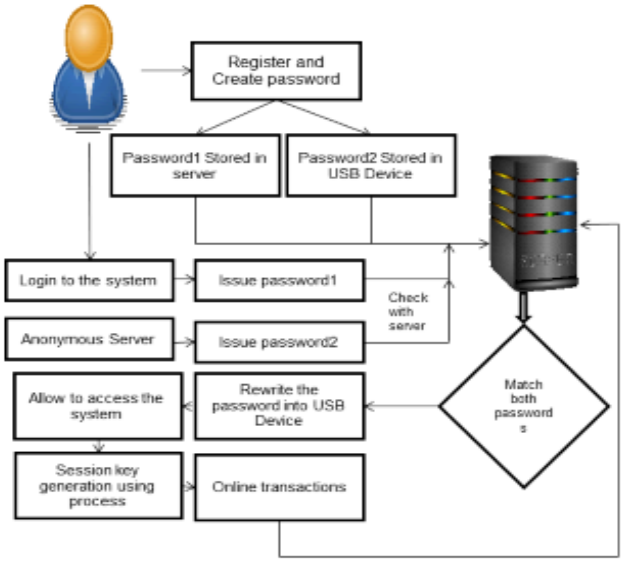

Fig. 1: Architecture for proposed work

5. CONCLUSION

In this work, proposed a novel Multi-Factor AKE scheme which preserves security against various attacks including de-synchronization attack, lost-smart-card attack, and password guessing attack, and helps several appropriate applications which include perfect forward secrecy, anonymity, adaptively password update, no centralized password storage and no long-time period public key. Furthermore, this protocol maintains high efficiency in terms of storage requirement, communication cost as well as computational complexity. This protocol requires only a few numbers of message flows and all the transmitted messages are short in size. Additional, the proposed scheme is provably secure in this extended security model of AKE. Therefore, the proposed approach is applicable for various low-power networks, in particular, the pervasive and mobile computing networks.

6. REFERENCES

[1] B.Wang and M. Ma, "A server independent authentication scheme for RFID systems," IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 689-696 Aug. 2012.

[2] 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.

[3] 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.

[4] G. Yang, D. S. Wong, H. Wang and X. Deng, "Two-factor mutual authentication based on smart cards and passwords," Journal of Computer and System Sciences, 74(7): 1160-1172, 2008.

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

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

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

[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 System", Wireless Personal Communications, October 2015, Volume 84, Issue 4, pp. 2571–2598.

[9] Virlla Devi Soothar, "Three Party Authentication Scheme for Rfid Systems in IOT" July 2017.

[10] 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.

