Immune Distinctive Authentication for E-transaction through Remote Systems

Sudeep.V
SITE, VIT University.
Vellore, Tamil Nadu, India

Pradeep Freddy. A
SITE, VIT University.
Vellore, Tamil Nadu, India

Avinash Choudhary. A.R
SITE, VIT University
Vellore, Tamil Nadu, India

ABSTRACT

Fast development in Information Communication Technology (ICT) and cellular telephone innovations empower users to perform online transactions from cell telephones/machines from anyplace, at whenever. Thus users need to oversee various online records. Thusly users key-in numerous login data to verify/access them. Consequently it is troublesome for users to oversee various online record accreditations. Presently users plan to have basic qualifications for all the online records or store them in a content document in cellular telephone and physically get to the record at whatever point they require login certifications. This is a genuine security danger for users, who are more helpless against certifications theft because of spying, shoulder surfing when they perform transactions at un-purified environment, for example, open web joint. In this paper we actualize a novel validation plan Immune Distinctive Authentication for E-Transactions Through Remote Systems (IDAERS) - Identity Based Elliptic Curve Encryption method which encourages users without breaking a sweat to work various online record transaction verification without the need to recall qualifications on cellular telephone gadget.

Index Terms:

E-Transactions, Elliptic Curve Encryption, Information Communication Technology , Identity Based, Remote Systems, public key generator(PKG).

1. INTRODUCTION

The growth of Information Communication Technology has motivated the users to perform their transactions over internet with the help of smart devices, desktops, laptops and etc. Due to the revolution in the area of operating system developments and smart devices, catalyzed the service providers such as social media, insurance, banking sector and their customers etc., to develop plethora of smart Applications and consequently increase the online e-commerce transactions through smart devices. In order to perform these transactions, a user has to enter his/her credentials for authorization and authentication. Biggest challenge and concern a user confronts is to remember and manage many of his credentials**.** In order to overcome this, users are tend to keep common credentials for all their transactions, or storing them in a text file or writing it down on a paper etc. which is a prone to security threat. The intruders can steal the credentials or may perform adverse operations. Nevertheless shoulder surfing is a potential security threat mostly in un-sanitized public places which ends up revealing the credentials to hackers. Here the intruders can reveal them by spying the typing pattern or either camera scanning, etc. There are many instances where user identity and credentials thefts are reported worldwide. As a result users may end up losing trust in online transactions.

These problems are addressed in many ways such as desktop Password Manager Application, storing the credentials as Mobile key chain applications and bookmark in cache. These remedies addresses well in a sanitized environment but are not applicable for un-sanitized environment. Moreover, Cloud based password management solutions can be used which enable credentials access from anywhere, at any time. Nevertheless this raises trustworthiness issues to outsource the personal credentials management to third party, also such services are too expensive. To overcome the above discussed threats, we propose less infrastructure, low cost, novel viable application for mobile phone device, wherein the user can store credentials of his\her online accounts securely and later use them to perform e-transactions on a public domain system without any manual intervention through Bluetooth.

2. RELATED WORK

Cell phone requisitions are created which confirms client onto online record on the same Brilliant gadget. Program plugins introduced on particular desktop/smart phone use stored qualifications which will confirm client consequently for e-transactions. The desktop watchword supervisor results are limited provisions which store qualifications on the hard-drive or utilize level document framework. The Cloud based secret word administration result gives intends to get to the qualifications anyplace, at whenever yet it is not a great choice to store accreditations in the outsider databases. The methodologies examined don't address the security dangers for the situation wherein client performs e-transaction in the earth. To address this we propose structural planning Immune Distinctive Authentication for E-Transactions Through Remote Systems (IDAERS) which utilizes Identity Based Elliptic bend cryptography (IBE) plan which is all the more compelling cryptographic plan when contrasted with others; for encryption, and unscrambling, which unravels the constraints.

3. SYSTEM DESIGN OF IDAERS

The IDAERS architecture (Fig 1), consists of remote devices; which is used to cache the account credentials which is in encrypted form .The mobile devices which is deployed with software agent which serves as listener to request from users. The mobile device agent co-ordinates with local PKG to launch online account, and it have a privileged access to native APIs to use services provided by system. To carryout e-transaction from mobile phone in unsafe environment through remote desktop the following sequence of operation are performed.

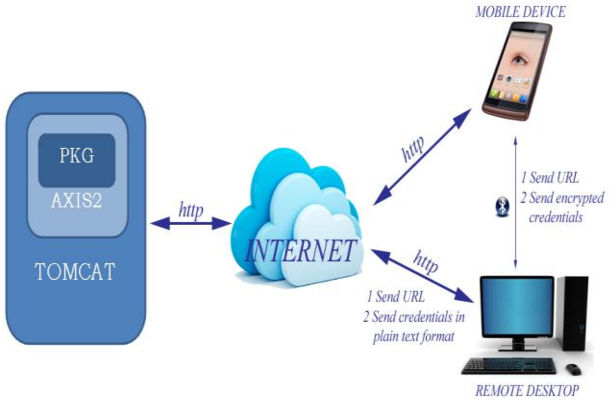

Fig 1: Architecture of IDAERS

User's Credentials for different accounts are securely stored in encrypted format by using dynamic pin(IBE) on mobile device in a secured place and this serves as passVault (password vault). During transaction, the required credentials are decrypted by using a dynamic pin and the decrypted string is again encrypted by using public key of the mobile device and transferred using Bluetooth to remote device agent. Upon receiving the credentials the remote device agent decrypts credentials using private key which is used for carrying out the transaction. For cryptographic process like encryption, key generation and decryption, we make use of public key generator (PKG) which is IBE based and installed in centralized server. In order to carry out encryption and decryption, System fetches cryptographic key and parameters from PKG using http protocol. REST architecture is used by PKG to provide cryptographic services (see Table 1).

Table 1: Services Offered by PKG

Serial *Number*	*Service*	*Functionality*
1	*Maps Keys getKeys(String UniqueDeviceID)*	*Returns the public and private keys*
2	*String cipherDatagetEncyptedData(String publicKey, String data)*	*Encrypts the data with given public key and returns the encypted data*
3	*String plainDatagetDecryptedData(String privateKey, String data)*	*Decrypts the data with given private key and returns the plain data.*

The Password Vault is deployed on mobile platform. The Passvault modules include: Account management, communication management and Application management. Application Profile Management: The profile management module is used to authenticate the user's credentials on the mobile phone device. This module provides application level security. The user needs to provide the user name, user password, and the dynamic pin during singing up the application profile for the first time and whenever the application is used again.

The dynamic pin security parameter is user selected. This pin can be either an alpha numeric or biometric parameter like retina scan, finger prints and for security reasons these pin are not stored on the device. The dynamic pin is used by application only on serve basis or on demand. The following are the steps to show the application profile information being encrypted and stored on mobile device securely. Local PKG generates application public key by using the dynamic pin. The Local PKG uses public key to encrypt application user name and password by IBE-ECC technique and stores the encrypted data in application memory which is restricted and secured. Profile management authorizes the user upon start of password vault. Local PKG uses dynamic pin to generate the private key and used for decryption of application user name and password which was earlier encrypted and authorizes user to use the password vault.

Account Management: This module is used by the user to modify his account credentials like add, edit and delete the user name and the user password. During these account management operations, the user should provide the dynamic pin for the application to carry out encryption and decryption which is done using IBE technique as shown in figure 2 and figure 3.

4. COMMUNICATION PROTOCOL

We propose an unique protocol to enable the secure transmission of user credentials from a mobile device to a remote system. This protocol has 2 phases: they are Mutual Authentication validation phase and immune remote login. In mutual authentication also known as two-way authentication both the parties authenticate each other at a time, here user/client authorizes by own to server and the server authorizes itself to user by knowing each other identity. are Mutual Authentication validation is used only in need of extra layer of security, usually in between organizations for financial transaction. Enhanced organization-to-client authorization will avert invaders from successfully satirizing financial organizations to snip clients' account credentials and improved client-to-organization authorization will inhibit invaders from successfully satirizing clients to financial organizations in order to commit racket.

Mutual Authentication Validation:

This phase incorporates validation with mutual authentication using Identity based Elliptical Curve Cryptography Technique. The figure given below depicts the validation mechanism between the mobile device and the remote system.

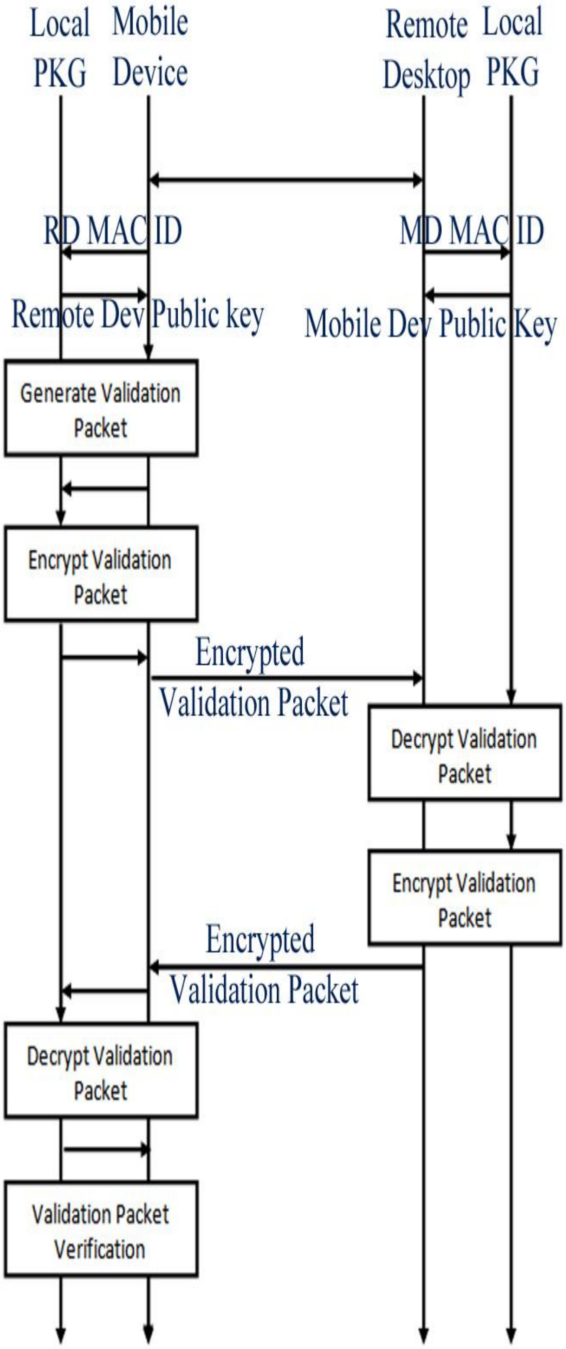
Local PKG
Mobile Device
Remote Desktop
Local PKG
RD MAC ID
MD MAC ID
Remote Dev Public key
Mobile Dev Public Key
Generate Validation Packet
Encrypt Validation Packet
Encrypted Validation Packet
Decrypt Validation Packet
Encrypt Validation Packet
Encrypted Validation Packet
Decrypt Validation Packet
Validation Packet Verification

Fig 2: Validation of Agents

Immune Remote Login

In this phase, first, the mobile phone sends the URL in a plain text format to remote system. The remote system uses the system native API to launch the URL. Subsequently mobile device sends the encrypted personal credentials required for the transaction. The remote device then decrypts the credentials and passes them for user authentication. The figure given below describes the remote login process.

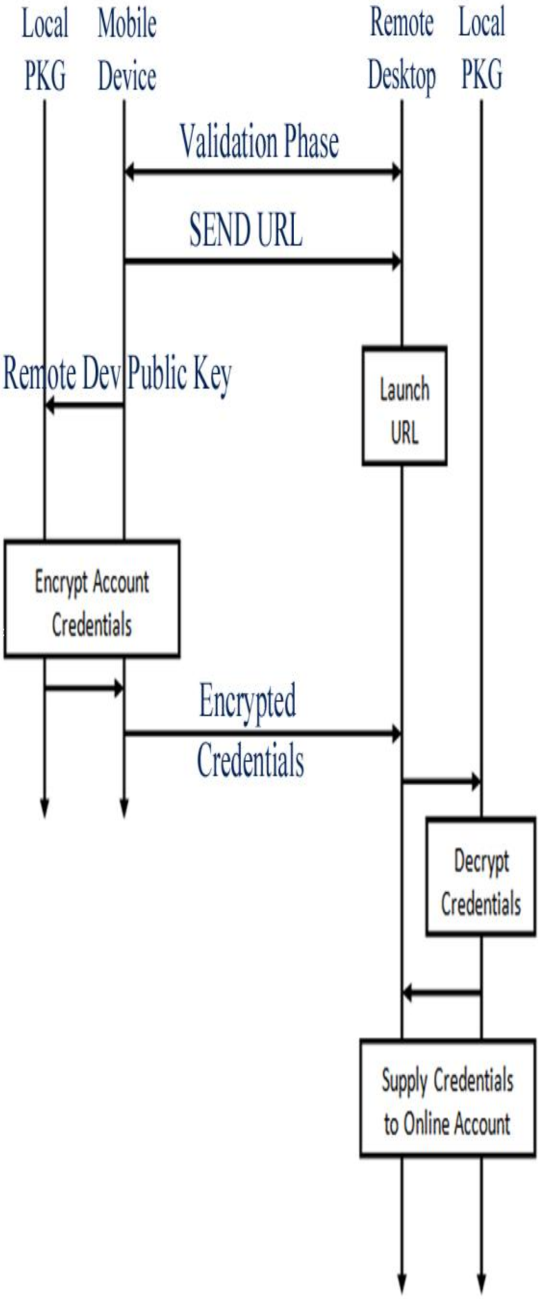

Fig 3: Credentials Transferred Securely

5. PERFORMANCE AND SECURITY ANALYSIS

The performance and the security analysis of this paper is done through exhaustive method in the below described sections.

5.1 Performance Analysis

The core functionality of IDAERS is centered at the cryptographic operations. Performance analysis of the cryptographic operations is estimated at both the Mobile device and the Remote Device (computer). The following table shows the performance evaluation of cryptographic operations.

Table 2: Results Of Performance Analysis

Functionality	**Device Type**	**Avg time is milliseconds**
Encryption	Remote Device	130
	Mobile Device	1706
Decryption	Remote Device	122
	Mobile Device	1570
Key Generation	Remote Device	87(PUB_KEY)
		104(PVT_KEY)
	Mobile Device	1739(PUB_KEY)
		2344(PVT_KEY)

5.2 Security Analysis:

5.2.1 Eaves Dropping: If in case the data is being hacked over the Bluetooth, the hacker will get to intercept the encrypted data. IDEARS proposed the use of Identity Based Encryption (IBE) to encrypt the data, this encrypted data is difficult to break; User Credential Redirection: The Remote Device is intelligent enough to identify to which account the information i.e the credentials is being passed to. The software agent hinders sending the credentials to the accounts which are other than the intended account.

5.2.2 Shoulder surfing: Hackers in some environments which are un-sanitized capture the keystrokes and try to re-use it. IDEARS solves this problem using wireless remote authentication.

5.2.3 Secure and Safe Bluetooth Communication: Even though the modes of transmission to transmit data is not safe and secure enough, IDEARS uses a message encryption using the IBE-ECC over Bluetooth.

5.2.4 Dacoity of Device: In case of device dacoity i.e theft, the contents present in the device is in an encrypted format which requires a dynamic pin to decrypt the credentials. IDEARS uses the IBE-ECC an encryption technique which is difficult to crack. However even if the dynamic pin is known by the thief, the entire system is vulnerable, this can be countered by using a biometric parameter as a dynamic pin which forms an 2 factor authorization.

5.2.5 Compromising the Remote Agent: If in case the remote device agent is being compromised, the MAC validation scheme will produce an error and hence the remote device agent can be identified or detected.

6. CONCLUSION AND FUTURE WORK

In this paper we have elucidated and designed IDEARS which works on an mobile device to authenticate in a secure way through Bluetooth on a Remote device. And have assessed the cryptographic operations of the Identity Based Encryption (IBE) scheme.

This technique can be further enhanced by making it work of different platforms and the problems regarding key revocation can be more explored in future. The implementation of this technique needs a thorough analysis in the area of security as it's the key functionality.

7. REFERENCES

[1] Olkowski, Jr and David,.J,.. Information Security Issues in E- Commerce 1 I, SANS GlAC Security Essentials, 2001.

[2] Raymond, G. Sin and Ramnath, K. Chellappa, , Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma, Information Technology and Management. 2005, p.181-202.

[3] Ramnath, K. Chellappa . Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security," http://asura.u sc.edu/ram/rcf-papers/sec- priv.pdf, 2001.

[4] Li Liu, Lei, Ming, Xiao,V, Vrbsky, Li, Chung Chih, and ,Yang, Susan. A Virtual Password Scheme to Protect Passwords. In Proceedings of the ICe. 2008, 1536-1540.

[5] CISCO, Implementing Keychain Management on Cisco lOS XR Software Cisco lOS XR System Security Configuration Guide.

[6] Danfeng Yao, Roberto, , Tamassia and Michael, T Goodrich, Notarized Federated Identity Management for Web Services. In: DSSec .2006, 133.

[7] R. Tamassia, D. Yao, and ,M. T. Goodrich, "Notarized Federated Identity Management for Web Services" http://www .cs. brown. edu/c gc/ stms/papers/notarizedFIM.p df, accessed July 2010.

[8] Dominique, Simon, Mayer , Ion, Guinard, Iulia and. In Search of an Internet of Things Service Architecture:REST or WS-*? A Developers' Perspective. In Proceedings of MobiQuitous. 2011.

[9] B S, Rajan, Adiga, Balamuralidhar, Shivraj V L, P Ravishankara, , M A, Shastry, and. Lightweight IBE Scheme for Wireless Sensor Nodes. In proceedings of IEEE ANTS 20 13(Accepted).