LIST OF FIGURES

2.1 Hash function properties using MD5…………………………… 12
2.2 Password Store used in Authentication……………………….. 13
2.3 Confidentiality and Authentication…………………………….. 15
2.4 Confidentiality and Integrity……………………………………… 15
2.5 Confidentiality using PKC………………………………………… 18
2.6 Authentication using PKC………………………………………… 18
2.7 Confidentiality and Integrity using PKC……………………….. 19
2.8 Public Key and Symmetric Key Encryption…………………… 20
2.9 Public Key and Symmetric Key Decryption………………….. 20
2.10 Digital Signature Creation and Verification………………….. 22
2.11 General format of X.509 v3 Digital Certificate……………….. 23
2.12 DHKE Protocol………………………………………………………. 26
2.13 Example of DHKE………………………………………………….. 26
2.14 MITM on DHKE……………………………………………………… 28
2.15 Screenshot of Online SBI Login page…………………………… 36
2.16 Screen shot of Bank of America online login page…………… 36
2.17 USB crypto token and RSA Secure ID…………………………. 39
2.18 Physiological & Behavioral Biometrics…………………………. 41
2.19 Contact Smart Card and pad layouts of Contact Card…….. 43
2.20 Architecture of Java Card Application…………………………. 45
2.21 Input of a DAS password in a 4x4 grid………………………… 74
2.22 DAS password and its system interpretation………………… 74
2.23 Grid Selection……………………………………………………….. 76
2.24 Signature drawing using mouse........................................ 76
2.25 Blonder's Graphical Password........................................ 78
2.26 PassPoints application interface.................................... 79
2.27 Dirik et al. predicted vs. actual click points...................... 80
2.28 User locating password using template.............................. 82
2.29 Example Login of Dèjà vu............................................. 83
2.30 Example of Convex Hull Click with 5 icons....................... 85
2.31 Setting code for variants of pass-objects.......................... 87
2.32 Example login screen of pass-objects............................... 87
2.33 Example interface of Authentigraph with characters.......... 89
2.34 Example interface of Authentigraph with shaped objects..... 89
2.35 VIP1/VIP2 Interface..................................................... 90
2.36 Example login interface of VIP3..................................... 90
2.37 Awase-E verification stage............................................ 93
2.38 Picture Password (Cats and Dogs theme).......................... 94
2.39 Example Login Interface of Passfaces............................. 97
2.40 myVidoop registration................................................. 99
2.41 Password Practice page................................................ 99
2.42 Password entry page................................................... 100
2.43 Activating the browser using activation code.................... 100
2.44 Flow of authentication data in ImageShield....................... 102
2.45 The Password Image (left) and Key Image (right)............. 104

3.1 Registration Phase.................................................... 116
3.2 Mutual Authentication & Key Agreement Phase.................. 117
3.3 Password Change Phase.............................................. 118
3.4 Screenshot of verification result

4.1 Example Image Grid for Login

4.2 Registration Phase

4.3 Mutual Authentication & Key Agreement Phase

4.4 Password Change Phase

4.5 Screenshot of verification result

5.1 Example Login Page of S-27

5.2 Registration Phase

5.3 Mutual Authentication & Key Agreement Phase

5.4 Password Change Phase

5.5 Example Login Page of S-16

5.6 Registration Phase

5.7 Mutual Authentication & Key Agreement Phase

5.8 Screenshot of verification result of S-27

5.9 Screenshot of verification result of S-16

6.1 Screen shot of STARS-27 Registration

6.2 Virtual Smart Card Download Page

6.3 Login Page displayed if Virtual Smart Card is found

6.4 Login Page displayed if the second factor is external device

6.5 Set Password page

6.6 User Profile page

6.7 Registration Success Page

6.8 Authentication & Session Key Generation page

6.9 Set Password Page of i-27

6.10 Set Password Page of i-16
6.11 Set Password page of S-27 ................................................. 200
6.12 Set Password page of S-16 ................................................. 200
6.13 Password Change option page ........................................... 204
6.14 Forget Password request page ............................................ 205
6.15 Secret Questions page ..................................................... 205
6.16 Password Reset page ..................................................... 206
6.17 Reloading of Smart Card Backup ........................................ 207
7.1 Total Number of Password Entries ........................................ 216
7.2 Strong Password Method .................................................. 217
7.3 Most Usable and Secure Password Method ......................... 217

LIST OF TABLES

2.1 Usability and Security comparison of various techniques... 109
3.1 Comparison of Functionality Analysis ................................. 121
3.2 Comparison of Computational Efficiency ........................... 122
4.1 Efficiency Analysis of Proposed Scheme ............................. 144
5.1 Efficiency comparison of S-27 and S-16 ............................. 181
7.1 Usability and Security Comparison of STARS ....................... 218

ABBREVIATIONS

SFA - Single-Factor Authentication
TFA - Two-Factor Authentication
MFA - Multi-Factor Authentication
FFIEC - Federal Financial Institutions Examining Council
POC - Proof of Concept
CIA - Confidentiality, Integrity, Authenticity
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAIN</td>
<td>Privacy, Authenticity, Integrity, Non-Repudiation</td>
</tr>
<tr>
<td>MD</td>
<td>Message Digest</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest Version 5</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hashing Algorithm</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Algorithm</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>PKC</td>
<td>Public Key Cryptography</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>DSC</td>
<td>Digital Signature Certificate</td>
</tr>
<tr>
<td>CCA</td>
<td>Controller of Certifying Authorities</td>
</tr>
<tr>
<td>CA</td>
<td>Certifying Authority</td>
</tr>
<tr>
<td>IT Act</td>
<td>Information Technology Act</td>
</tr>
<tr>
<td>DS</td>
<td>Digital Signature</td>
</tr>
<tr>
<td>DHKE</td>
<td>Diffie-Hellman Key Exchange</td>
</tr>
<tr>
<td>KEK</td>
<td>Key Encryption Key</td>
</tr>
<tr>
<td>MITM</td>
<td>Man-In-The-Middle</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, Adleman</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-Frequency Identification</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>ICC</td>
<td>Integrated Circuit Card</td>
</tr>
<tr>
<td>MULTOS</td>
<td>Multi-application Smart Card Operating System</td>
</tr>
<tr>
<td>PVC</td>
<td>Polyvinyl Chloride</td>
</tr>
<tr>
<td>ROI</td>
<td>Return on Investment</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
</tr>
<tr>
<td>PKCS</td>
<td>Public-Key Cryptography Standards</td>
</tr>
<tr>
<td>CSP</td>
<td>Cryptographic Service Provider</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>IDi</td>
<td>Identity (of User i)</td>
</tr>
<tr>
<td>PWi</td>
<td>Password (of User i)</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>XOR</td>
<td>Exclusive-OR Operation</td>
</tr>
<tr>
<td>FAQ</td>
<td>Frequently Asked Questions</td>
</tr>
</tbody>
</table>