# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER NO.</th>
<th>TITLE</th>
<th>PAGE NO.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ABSTRACT</td>
<td>viii</td>
</tr>
<tr>
<td></td>
<td>LIST OF TABLES</td>
<td>xvi</td>
</tr>
<tr>
<td></td>
<td>LIST OF FIGURES</td>
<td>xvii</td>
</tr>
<tr>
<td></td>
<td>LIST OF ABBREVIATIONS AND SYMBOLS</td>
<td>xix</td>
</tr>
<tr>
<td>1</td>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1</td>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.2</td>
<td>THE CLOUD LANDSCAPE</td>
<td>2</td>
</tr>
<tr>
<td>1.2.1</td>
<td>Cloud deployment models</td>
<td>2</td>
</tr>
<tr>
<td>1.2.2</td>
<td>Cloud services</td>
<td>3</td>
</tr>
<tr>
<td>1.3</td>
<td>CHALLENGES IN CLOUD COMPUTING</td>
<td>4</td>
</tr>
<tr>
<td>1.4</td>
<td>SECURITY ISSUES IN CLOUD COMPUTING</td>
<td>6</td>
</tr>
<tr>
<td>1.5</td>
<td>CLOUD SECURITY REQUIREMENTS</td>
<td>7</td>
</tr>
<tr>
<td>1.6</td>
<td>MOTIVATION OF RESEARCH</td>
<td>9</td>
</tr>
<tr>
<td>1.7</td>
<td>OBJECTIVE OF THE THESIS</td>
<td>12</td>
</tr>
<tr>
<td>1.8</td>
<td>THESIS CONTRIBUTIONS</td>
<td>12</td>
</tr>
<tr>
<td>1.8.1</td>
<td>Encryption for massive data storage in cloud</td>
<td>13</td>
</tr>
<tr>
<td>1.8.2</td>
<td>Data integrity proof and secure computation in cloud</td>
<td>13</td>
</tr>
<tr>
<td>1.8.3</td>
<td>Security for dynamic data storage in cloud</td>
<td>14</td>
</tr>
<tr>
<td>1.8.4</td>
<td>Remote user authentication using fingerprint in cloud</td>
<td>15</td>
</tr>
<tr>
<td>1.9</td>
<td>ORGANIZATION OF THE THESIS</td>
<td>15</td>
</tr>
<tr>
<td>2</td>
<td>LITERATURE SURVEY</td>
<td>18</td>
</tr>
<tr>
<td>2.1</td>
<td>INTRODUCTION</td>
<td>18</td>
</tr>
<tr>
<td>2.2</td>
<td>CLOUD COMPUTING AND SECURITY ISSUES – AN OVERVIEW</td>
<td>18</td>
</tr>
<tr>
<td>CHAPTER NO.</td>
<td>TITLE</td>
<td>PAGE NO.</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>2.3</td>
<td>ENCRYPTION FOR MASSIVE DATA STORAGE</td>
<td>20</td>
</tr>
<tr>
<td>2.4</td>
<td>DATA INTEGRITY PROOF AND SECURE COMPUTATION IN CLOUD</td>
<td>26</td>
</tr>
<tr>
<td>2.5</td>
<td>SECURED STORAGE FOR DYNAMIC DATA IN CLOUD</td>
<td>32</td>
</tr>
<tr>
<td>2.6</td>
<td>REMOTE USER AUTHENTICATION USING FINGERPRINT IN CLOUD</td>
<td>36</td>
</tr>
<tr>
<td>2.7</td>
<td>SUMMARY</td>
<td>40</td>
</tr>
<tr>
<td>3</td>
<td>ENCRYPTION FOR MASSIVE DATA STORAGE IN CLOUD</td>
<td>41</td>
</tr>
<tr>
<td>3.1</td>
<td>INTRODUCTION</td>
<td>41</td>
</tr>
<tr>
<td>3.2</td>
<td>SYSTEM MODEL FOR ENSURING CONFIDENTIALITY</td>
<td>42</td>
</tr>
<tr>
<td>3.3</td>
<td>SYSTEM OVERVIEW FOR 2-KEYS SYMMETRIC ENCRYPTION</td>
<td>43</td>
</tr>
<tr>
<td>3.4</td>
<td>ENSURING CONFIDENTIALITY</td>
<td>45</td>
</tr>
<tr>
<td>3.4.1</td>
<td>2-Keys symmetric encryption</td>
<td>45</td>
</tr>
<tr>
<td>3.4.1.1</td>
<td>Generation of binary sequence</td>
<td>47</td>
</tr>
<tr>
<td>3.4.1.2</td>
<td>Key generation</td>
<td>48</td>
</tr>
<tr>
<td>3.4.1.3</td>
<td>Data encryption</td>
<td>50</td>
</tr>
<tr>
<td>3.4.1.4</td>
<td>Data decryption</td>
<td>51</td>
</tr>
<tr>
<td>3.5</td>
<td>SIMULATION AND RESULTS</td>
<td>55</td>
</tr>
<tr>
<td>3.6</td>
<td>CRYPTANALYSIS</td>
<td>59</td>
</tr>
<tr>
<td>3.6.1</td>
<td>Security model for confidentiality</td>
<td>59</td>
</tr>
<tr>
<td>3.6.2</td>
<td>Security attacks</td>
<td>60</td>
</tr>
<tr>
<td>3.7</td>
<td>PERFORMANCE ANALYSIS</td>
<td>66</td>
</tr>
<tr>
<td>3.7.1</td>
<td>Complexity of encryption function</td>
<td>66</td>
</tr>
<tr>
<td>3.7.2</td>
<td>Encryption and decryption time</td>
<td>67</td>
</tr>
<tr>
<td>3.8</td>
<td>SUMMARY</td>
<td>70</td>
</tr>
<tr>
<td>CHAPTER NO.</td>
<td>TITLE</td>
<td>PAGE NO.</td>
</tr>
<tr>
<td>-------------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>4</td>
<td>DATA INTEGRITY PROOF AND SECURE COMPUTATION IN CLOUD COMPUTING</td>
<td>71</td>
</tr>
<tr>
<td>4.1</td>
<td>INTRODUCTION</td>
<td>71</td>
</tr>
<tr>
<td>4.2</td>
<td>SYSTEM MODEL FOR DATA INTEGRITY ASSURANCE</td>
<td>73</td>
</tr>
<tr>
<td>4.3</td>
<td>FUNCTIONS FOR ASSURING DATA AND COMPUTATION INTEGRITY</td>
<td>74</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Data integrity assurance</td>
<td>74</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Computation security assurance</td>
<td>75</td>
</tr>
<tr>
<td>4.4</td>
<td>ASSURING THE INTEGRITY OF DATA AND COMPUTATION</td>
<td>77</td>
</tr>
<tr>
<td>4.4.1</td>
<td>Stored data integrity assurance</td>
<td>77</td>
</tr>
<tr>
<td>4.4.2</td>
<td>Computation security</td>
<td>82</td>
</tr>
<tr>
<td>4.5</td>
<td>RESULTS AND DISCUSSION</td>
<td>88</td>
</tr>
<tr>
<td>4.6</td>
<td>SECURITY ANALYSIS</td>
<td>91</td>
</tr>
<tr>
<td>4.6.1</td>
<td>Security model for assuring integrity</td>
<td>91</td>
</tr>
<tr>
<td>4.6.2</td>
<td>Ensuring data integrity</td>
<td>92</td>
</tr>
<tr>
<td>4.7</td>
<td>PERFORMANCE ANALYSIS</td>
<td>96</td>
</tr>
<tr>
<td>4.7.1</td>
<td>Time for metadata generation</td>
<td>96</td>
</tr>
<tr>
<td>4.7.2</td>
<td>Storage cost</td>
<td>98</td>
</tr>
<tr>
<td>4.7.3</td>
<td>Computation cost</td>
<td>99</td>
</tr>
<tr>
<td>4.7.4</td>
<td>Communication cost</td>
<td>100</td>
</tr>
<tr>
<td>4.8</td>
<td>SUMMARY</td>
<td>101</td>
</tr>
<tr>
<td>5</td>
<td>REMOTE USER AUTHENTICATION USING FINGERPRINT IN CLOUD</td>
<td>103</td>
</tr>
<tr>
<td>5.1</td>
<td>INTRODUCTION</td>
<td>103</td>
</tr>
<tr>
<td>5.2</td>
<td>OVERVIEW OF EXISTING AUTHENTICATION METHODS</td>
<td>103</td>
</tr>
<tr>
<td>5.3</td>
<td>SYSTEM OVERVIEW FOR REMOTE AUTHENTICATION</td>
<td>106</td>
</tr>
<tr>
<td>5.3.1</td>
<td>Setup phase</td>
<td>106</td>
</tr>
<tr>
<td>CHAPTER NO.</td>
<td>TITLE</td>
<td>PAGE NO.</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Initialization phase</td>
<td>106</td>
</tr>
<tr>
<td>5.3.3</td>
<td>Registration phase</td>
<td>106</td>
</tr>
<tr>
<td>5.3.4</td>
<td>Authentication phase</td>
<td>107</td>
</tr>
<tr>
<td>5.4</td>
<td>REMOTE USER AUTHENTICATION</td>
<td>108</td>
</tr>
<tr>
<td>5.4.1</td>
<td>Operations for initiating authenticity</td>
<td>108</td>
</tr>
<tr>
<td>5.4.2</td>
<td>Sequence of operations for data/service access</td>
<td>109</td>
</tr>
<tr>
<td>5.4.3</td>
<td>Architectural model for remote authentication</td>
<td>110</td>
</tr>
<tr>
<td>5.4.3.1</td>
<td>Initialization phase</td>
<td>111</td>
</tr>
<tr>
<td>5.4.3.2</td>
<td>Registration phase</td>
<td>119</td>
</tr>
<tr>
<td>5.4.3.3</td>
<td>Authentication phase</td>
<td>121</td>
</tr>
<tr>
<td>5.5</td>
<td>SECURITY ANALYSIS</td>
<td>126</td>
</tr>
<tr>
<td>5.5.1</td>
<td>Security model for remote authentication</td>
<td>126</td>
</tr>
<tr>
<td>5.5.2</td>
<td>Security attacks</td>
<td>126</td>
</tr>
<tr>
<td>5.6</td>
<td>PERFORMANCE MEASUREMENT</td>
<td>129</td>
</tr>
<tr>
<td>5.6.1</td>
<td>Accuracy and error rate</td>
<td>129</td>
</tr>
<tr>
<td>5.6.2</td>
<td>Storage cost</td>
<td>130</td>
</tr>
<tr>
<td>5.6.3</td>
<td>Computation cost</td>
<td>131</td>
</tr>
<tr>
<td>5.6.4</td>
<td>Communication cost</td>
<td>132</td>
</tr>
<tr>
<td>5.6.5</td>
<td>Time complexity</td>
<td>133</td>
</tr>
<tr>
<td>5.7</td>
<td>SUMMARY</td>
<td>134</td>
</tr>
<tr>
<td>6</td>
<td>CIA MODEL FOR DYNAMIC DATA STORAGE IN CLOUD</td>
<td>136</td>
</tr>
<tr>
<td>6.1</td>
<td>CIA SECURITY MODEL</td>
<td>136</td>
</tr>
<tr>
<td>6.2</td>
<td>DYNAMIC DATA STORAGE SECURITY</td>
<td>137</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Construction of linked list</td>
<td>137</td>
</tr>
<tr>
<td>6.2.2</td>
<td>Block insertion</td>
<td>138</td>
</tr>
<tr>
<td>6.2.3</td>
<td>Block modification</td>
<td>139</td>
</tr>
<tr>
<td>6.2.4</td>
<td>Block appending</td>
<td>139</td>
</tr>
<tr>
<td>CHAPTER NO.</td>
<td>TITLE</td>
<td>PAGE NO.</td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>6.2.5</td>
<td>Block deletion</td>
<td>140</td>
</tr>
<tr>
<td>6.3</td>
<td>CIA MODEL</td>
<td>140</td>
</tr>
<tr>
<td>6.3.1</td>
<td>Sequence of operations in CIA model</td>
<td>142</td>
</tr>
<tr>
<td>6.4</td>
<td>SECURITY ANALYSIS FOR CIA MODEL</td>
<td>143</td>
</tr>
<tr>
<td>6.4.1</td>
<td>Security model</td>
<td>143</td>
</tr>
<tr>
<td>6.4.2</td>
<td>Confidentiality</td>
<td>144</td>
</tr>
<tr>
<td>6.4.3</td>
<td>Integrity</td>
<td>144</td>
</tr>
<tr>
<td>6.4.4</td>
<td>Authentication</td>
<td>144</td>
</tr>
<tr>
<td>6.5</td>
<td>PERFORMANCE COMPARISON</td>
<td>144</td>
</tr>
<tr>
<td>6.6</td>
<td>SUMMARY</td>
<td>149</td>
</tr>
<tr>
<td>7</td>
<td>CONCLUSION AND FUTURE ENHANCEMENT</td>
<td>150</td>
</tr>
<tr>
<td>7.1</td>
<td>CONCLUSION</td>
<td>150</td>
</tr>
<tr>
<td>7.2</td>
<td>FUTURE WORKS</td>
<td>151</td>
</tr>
<tr>
<td>REFERENCES</td>
<td></td>
<td>152</td>
</tr>
<tr>
<td>LIST OF PUBLICATIONS</td>
<td></td>
<td>161</td>
</tr>
<tr>
<td>TECHNICAL BIOGRAPHY</td>
<td></td>
<td>162</td>
</tr>
<tr>
<td>TABLE NO.</td>
<td>TITLE</td>
<td>PAGE NO.</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>3.1</td>
<td>Encryption and decryption time for different file sizes</td>
<td>68</td>
</tr>
<tr>
<td>3.2</td>
<td>Encryption time for the existing and proposed 2-Keys symmetric encryption algorithm</td>
<td>69</td>
</tr>
<tr>
<td>4.1</td>
<td>Hardware configuration required for eucalyptus cloud environment setup</td>
<td>88</td>
</tr>
<tr>
<td>4.2</td>
<td>Metadata values for the text “cloud computing”</td>
<td>90</td>
</tr>
<tr>
<td>4.3</td>
<td>Probability of detection Pd of data replacement corruptions for 1000 blocks, 20 sectors in a block and 1 corrupted block.</td>
<td>94</td>
</tr>
<tr>
<td>4.4</td>
<td>Time requirement for generation of metadata and inverse of metadata for different data file sizes</td>
<td>97</td>
</tr>
<tr>
<td>4.5</td>
<td>Cost of computation and storage overhead at DO, TPA and server</td>
<td>100</td>
</tr>
<tr>
<td>5.1</td>
<td>Sample pixel intensity differences indicating the edges</td>
<td>113</td>
</tr>
<tr>
<td>5.2</td>
<td>Sibling information required for generating signature Sequence of operations in the registration phase</td>
<td>120</td>
</tr>
<tr>
<td>5.3</td>
<td>Measure of accuracy and error rate for a sample of 50 images</td>
<td>130</td>
</tr>
<tr>
<td>6.1</td>
<td>Summary of storage and computation cost for CIA model</td>
<td>145</td>
</tr>
<tr>
<td>6.2</td>
<td>Comparison of proposed CIA model with the existing approaches</td>
<td>148</td>
</tr>
</tbody>
</table>
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE NO.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>CIA triad</td>
<td>11</td>
</tr>
<tr>
<td>2.1</td>
<td>Taxonomy of encryption algorithms</td>
<td>21</td>
</tr>
<tr>
<td>3.1</td>
<td>System model for ensuring confidentiality</td>
<td>43</td>
</tr>
<tr>
<td>3.2</td>
<td>Architecture of 2-Keys symmetric encryption algorithm</td>
<td>47</td>
</tr>
<tr>
<td>3.3</td>
<td>Operation sequence for encryption</td>
<td>54</td>
</tr>
<tr>
<td>3.4</td>
<td>Operation sequence for decryption</td>
<td>55</td>
</tr>
<tr>
<td>3.5</td>
<td>Binary sequence</td>
<td>57</td>
</tr>
<tr>
<td>3.6</td>
<td>Data file F (Plain text)</td>
<td>58</td>
</tr>
<tr>
<td>3.7</td>
<td>Encrypted data file (Cipher text)</td>
<td>59</td>
</tr>
<tr>
<td>3.8</td>
<td>Frequency of English alphabets</td>
<td>63</td>
</tr>
<tr>
<td>3.9</td>
<td>Frequency of characters in plain text</td>
<td>64</td>
</tr>
<tr>
<td>3.10</td>
<td>Frequency of characters in cipher text</td>
<td>65</td>
</tr>
<tr>
<td>3.11</td>
<td>Comparison of encryption time of standard encryption algorithms with the 2-Keys symmetric encryption algorithm</td>
<td>68</td>
</tr>
<tr>
<td>4.1</td>
<td>System model for data integrity assurance</td>
<td>74</td>
</tr>
<tr>
<td>4.2</td>
<td>System architecture for ensuring data integrity</td>
<td>79</td>
</tr>
<tr>
<td>4.3</td>
<td>Format of data blocks stored in cloud</td>
<td>82</td>
</tr>
<tr>
<td>4.4</td>
<td>Merkle hash tree constructed by the cloud server</td>
<td>83</td>
</tr>
<tr>
<td>4.5</td>
<td>Architecture for ensuring computation integrity</td>
<td>85</td>
</tr>
<tr>
<td>4.6</td>
<td>Merkle hash tree with dummy nodes</td>
<td>87</td>
</tr>
<tr>
<td>4.7</td>
<td>Probability of detection Pd of data replacement corruptions for 1000 blocks, 20 sectors in a block</td>
<td>95</td>
</tr>
<tr>
<td>4.8</td>
<td>Probability of detection Pd of corruptions like data replacement, insertion, deletion and appending on the data of 1000 blocks, 20 sectors in a block and 1 corrupted block</td>
<td>96</td>
</tr>
<tr>
<td>4.9</td>
<td>Time requirement of metadata generation and generation of inverse of metadata for different data file sizes</td>
<td>98</td>
</tr>
<tr>
<td>FIGURE NO.</td>
<td>TITLE</td>
<td>PAGE NO.</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>4.10</td>
<td>Comparison of the storage size of the data with metadata and without</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>metadata</td>
<td></td>
</tr>
<tr>
<td>5.1</td>
<td>Flow of messages for secured authentication</td>
<td>110</td>
</tr>
<tr>
<td>5.2</td>
<td>Architectural model for remote user authentication</td>
<td>111</td>
</tr>
<tr>
<td>5.3</td>
<td>Fingerprint images after the image enhancement operations</td>
<td>114</td>
</tr>
<tr>
<td>5.4</td>
<td>Binarized image and its equal shares</td>
<td>114</td>
</tr>
<tr>
<td>5.5</td>
<td>Merkle Hash tree generated from the hash values of the fingerprint</td>
<td>117</td>
</tr>
<tr>
<td></td>
<td>shares</td>
<td></td>
</tr>
<tr>
<td>5.6</td>
<td>Sequence of operations in the registration phase</td>
<td>120</td>
</tr>
<tr>
<td>5.7</td>
<td>Construction of Merkle hash tree from the adjacent fingerprint shares</td>
<td>124</td>
</tr>
<tr>
<td>5.8</td>
<td>Sequence of operations in the authentication phase</td>
<td>125</td>
</tr>
<tr>
<td>5.9</td>
<td>Variation of storage cost of DU, DO and CSP</td>
<td>131</td>
</tr>
<tr>
<td>5.10</td>
<td>Variation of messages exchanged between DU, DO and CSP</td>
<td>132</td>
</tr>
<tr>
<td>5.11</td>
<td>Time of execution of image enhancement operations at the data user</td>
<td>133</td>
</tr>
<tr>
<td>6.1</td>
<td>Linked list construction</td>
<td>137</td>
</tr>
<tr>
<td>6.2</td>
<td>Linked list after block insertion</td>
<td>139</td>
</tr>
<tr>
<td>6.3</td>
<td>Linked list after block appending</td>
<td>140</td>
</tr>
<tr>
<td>6.4</td>
<td>Linked list after deletion of a block</td>
<td>140</td>
</tr>
<tr>
<td>6.5</td>
<td>Architecture for CIA model</td>
<td>141</td>
</tr>
<tr>
<td>6.6</td>
<td>Probability of detection (Pd) of data insertion, deletion, appending</td>
<td>146</td>
</tr>
<tr>
<td></td>
<td>corruptions for 1000 blocks, 20 sectors in a block and 1 corrupted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>block</td>
<td></td>
</tr>
<tr>
<td>6.7</td>
<td>Probability of detection (Pd) of data replacement</td>
<td>147</td>
</tr>
<tr>
<td></td>
<td>corruptions for 100 blocks, 10 sectors in a block and 1 corrupted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>block</td>
<td></td>
</tr>
</tbody>
</table>
### LIST OF ABBREVIATIONS AND SYMBOLS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-DES</td>
<td>Triple Data Encryption Standard</td>
</tr>
<tr>
<td>ACID</td>
<td>Atomicity, Consistency, Isolation and Duration</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ASCII</td>
<td>American Standard Code for Information Interchange</td>
</tr>
<tr>
<td>AV</td>
<td>Authentication Values</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CAM</td>
<td>Cloud Access Management</td>
</tr>
<tr>
<td>CC</td>
<td>Computation Cost</td>
</tr>
<tr>
<td>CFB</td>
<td>Cipher Feedback</td>
</tr>
<tr>
<td>CIA</td>
<td>Confidentiality, Integrity and Authentication</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Relationship Management</td>
</tr>
<tr>
<td>CSA</td>
<td>Cloud Security Alliance</td>
</tr>
<tr>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>DAC</td>
<td>Discretionary Access Control</td>
</tr>
<tr>
<td>DB</td>
<td>Data Block</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DO</td>
<td>Data Owner</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DPDP</td>
<td>Dynamic Provable Data Possession</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
</tr>
<tr>
<td>DU</td>
<td>Data User</td>
</tr>
<tr>
<td>ECB</td>
<td>Electronic Code Book</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
</tr>
<tr>
<td>EDB</td>
<td>Encrypted Data Block</td>
</tr>
<tr>
<td>F</td>
<td>Data File</td>
</tr>
<tr>
<td>FHE</td>
<td>Fully Homomorphic Encryption</td>
</tr>
<tr>
<td>FN</td>
<td>False Negative</td>
</tr>
<tr>
<td>FP</td>
<td>False Positive</td>
</tr>
<tr>
<td>FPS</td>
<td>Finger Print Share</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>HLA</td>
<td>Homomorphic Linear Authenticator</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hash Message Authentication Code</td>
</tr>
<tr>
<td>HRM</td>
<td>Human Resource Management</td>
</tr>
<tr>
<td>HVT</td>
<td>Homomorphic Verifiable Tag</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>IC</td>
<td>Initial Coefficient</td>
</tr>
<tr>
<td>IRF</td>
<td>Inverse Random Function</td>
</tr>
<tr>
<td>ISK</td>
<td>Intermediate Session Key</td>
</tr>
<tr>
<td>i</td>
<td>Block position in the data file</td>
</tr>
<tr>
<td>IV</td>
<td>Initialization Vector</td>
</tr>
<tr>
<td>j</td>
<td>Character position in a data block</td>
</tr>
<tr>
<td>KB</td>
<td>Kilo Bytes</td>
</tr>
<tr>
<td>KW1</td>
<td>Keyword1</td>
</tr>
<tr>
<td>KW2</td>
<td>Keyword2</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>m</td>
<td>Initial seed for binary sequence generation</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>mb</td>
<td>Modified Data Blocks</td>
</tr>
<tr>
<td>MB</td>
<td>Mega Bytes</td>
</tr>
<tr>
<td>MDB</td>
<td>Meta data Block</td>
</tr>
<tr>
<td>MHT</td>
<td>Merkle Hash Tree</td>
</tr>
<tr>
<td>ms</td>
<td>Millisecond</td>
</tr>
<tr>
<td>n</td>
<td>Number of bytes in a block</td>
</tr>
<tr>
<td>nb</td>
<td>Number of data blocks</td>
</tr>
<tr>
<td>n-PCDH</td>
<td>n-Power Computational Diffie Hellman</td>
</tr>
<tr>
<td>OFB</td>
<td>Output Feedback</td>
</tr>
<tr>
<td>P</td>
<td>Position of the data block</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>Pd</td>
<td>Probability of Detection of Data Corruption</td>
</tr>
<tr>
<td>PDDP</td>
<td>Provable Dynamic Data Possession</td>
</tr>
<tr>
<td>PDP</td>
<td>Provable Data Possession</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>PoR</td>
<td>Proof of Retrievability</td>
</tr>
<tr>
<td>PPDP</td>
<td>Proxy Provable Data Possession</td>
</tr>
<tr>
<td>q</td>
<td>Initial value for key exchange</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>randno</td>
<td>Randomly Chosen Integer</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role Based Access Control</td>
</tr>
<tr>
<td>RBASL</td>
<td>Rank Based Authenticated Skip List</td>
</tr>
<tr>
<td>RC2</td>
<td>Rivest Cipher 2</td>
</tr>
<tr>
<td>RC4</td>
<td>Rivest Cipher 4</td>
</tr>
<tr>
<td>RF</td>
<td>Random Function</td>
</tr>
<tr>
<td>RMI</td>
<td>Remote Method Invocation</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest Shamir Adleman</td>
</tr>
<tr>
<td>S3</td>
<td>Simple Storage Service</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>s-HTTP</td>
<td>Secure HyperText Transfer Protocol</td>
</tr>
<tr>
<td>Sk</td>
<td>Secret key</td>
</tr>
<tr>
<td>SK</td>
<td>Session Key</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign On</td>
</tr>
<tr>
<td>t</td>
<td>Number of Challenges</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TN</td>
<td>True Negative</td>
</tr>
<tr>
<td>TNR</td>
<td>True Negative Rate</td>
</tr>
<tr>
<td>TOK</td>
<td>Token</td>
</tr>
<tr>
<td>TP</td>
<td>True Positive</td>
</tr>
<tr>
<td>TPA</td>
<td>Third Party Auditor</td>
</tr>
<tr>
<td>TPR</td>
<td>True Positive Rate</td>
</tr>
<tr>
<td>UEC</td>
<td>Ubuntu Enterprise Cloud</td>
</tr>
<tr>
<td>v</td>
<td>Noise Variance</td>
</tr>
<tr>
<td>x</td>
<td>An integer value</td>
</tr>
<tr>
<td>XA, XB</td>
<td>A random number chosen for key exchange</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>XOR</td>
<td>Exclusive-OR</td>
</tr>
<tr>
<td>y</td>
<td>An integer value</td>
</tr>
<tr>
<td>α</td>
<td>Initial value for key exchange</td>
</tr>
<tr>
<td>σ</td>
<td>Mean Variance</td>
</tr>
<tr>
<td>Ω</td>
<td>Signature</td>
</tr>
<tr>
<td>μ</td>
<td>Local Variance</td>
</tr>
<tr>
<td>β</td>
<td>Integer relatively prime to y and α</td>
</tr>
</tbody>
</table>