

**AN EFFICIENT SCHEME FOR SOCIAL NETWORK  
MODEL USING A DYNAMIC AUTHENTICATION  
PROTOCOL TECHNIQUE**

Thesis Submitted for the Award of the Degree of

**DOCTOR OF PHILOSOPHY**

in

**Computer Science & Engineering**

By

**Vivek Kumar Sinha**

**Registration Number: 41700221**

**Supervised By**

**Dr. Divya**

**Assistant Professor**

**Computer Science & Engineering**

**Lovely Professional University, Punjab**



**L** OVELY  
**P** ROFESSIONAL  
**U** NIVERSITY

*Transforming Education Transforming India*

**LOVELY PROFESSIONAL UNIVERSITY, PUNJAB**

**2024**

## DECLARATION

I declare that the thesis entitled “**An Efficient Scheme for Social Network Model Using a Dynamic Authentication Protocol Technique**” has been prepared by me under the guidance of **Dr. Divya**, Assistant Professor, School of Computer Science and Engineering, Lovely Professional University. No part of this thesis has formed the basis for the award of any degree or fellowship previously.


Vivek Kumar Sinha

School of Computer Science and Engineering  
Lovely Professional University

Jalandhar-Delhi G.T.Road(NH1)

Phagwara, Punjab, India

Date: 18-07-2024



Signature of the Candidate

## CERTIFICATE

The research work embodied in the present Thesis entitled “An Efficient Scheme for Social Network Model Using a Dynamic Authentication Protocol Technique” has been carried out in the School of Computer Science and Engineering, Lovely Professional University, Phagwara Punjab. The work reported herein is original and does not form part of any other thesis or dissertation based on which a degree or award was conferred on an earlier occasion or to any other scholar.

I understand the University’s policy on plagiarism and declare that the thesis and publications are my work, except where specifically acknowledged, and have not been copied from other sources or been previously submitted for award or assessment.

**VIVEK KUMAR SINHA**

  
18.7.2024  
RESEARCH SCHOLAR

**Dr. DIVYA**

  
28.4.24  
SUPERVISOR

Assistant Professor

Department of Computer  
Science and Engineering

Lovely Professional  
University, Phagwara  
Punjab, India

## ACKNOWLEDGEMENT

At the very outset, I offer my sincere thanks to **Almighty God** for the grace and blessings that made me complete this research work. I sincerely thank my parents who have gifted me with this life to attain many achievements.

I am thankful to my guide **Dr. Divya** for her words of wisdom and guidance throughout my research work. Her knowledge about the domain helped me to travel through the tunnel of darkness and emerge victorious into the light. Her persistence for perfection helped me to improve my potential throughout my research work.

I am indebted to, the Chairman- Secretary, Lovely Professional University, Phagwara, and the Board of Members for their support. A special thanks to the Principal, Lovely Professional University, Phagwara, for providing me with the infrastructure to carry out the research.

My sincere thanks to the Correspondent of Lovely Professional University, Phagwara for his support in helping me to reach my goals. I am indebted to my colleagues for their moral support.

I am forever grateful to my father, mother, brother, wife, and son for their support and encouragement. Their understanding helped me to complete my work without inhibitions.

**VIVEK KUMAR SINHA**

## ABSTRACT

Security and privacy of user data in social network settings are constantly becoming a very key challenge all across the globe. The usage of social networks has increased very rapidly during the past few years owing to various factors such as technological infrastructure development, increment in global population, rise in smartphone users including the internet, etc. During the last decade, multifarious investigators have developed multifarious methods to provide the required secrecy during dataset transmission over social networks. Larger-scale social networks have made this necessary for two communicating members to exchange the meeting credentials using a distant server to connect safely. Owing to the rapid technical upgradation in the information technology (IT) setup and multiple applications, internet subscribers are increasingly concerned with the translation of diverse confidential information contained in pictures, text messaging, and videos as means of social networks in day-to-day life. Furthermore, the secrecy and confidentiality of such secured information have many confidentiality risks in real-time transmissions owing to multiple assaults namely cryptanalysis, man-in-the-middle replay attacks, etc.

There are diverse widely popular methods developed by the researchers such as trust as well as a repudiation of multistage user authentication. Trust and repudiation are widely used techniques in multiphase authentication of users. The trust has mainly recognized a group of authorization and authentication that deals with diverse techniques to facilitate access control, thereby, offering trust-associated solutions. Privacy and secrecy can be evaluated based on these diverse four elements namely access, as well as capturing, control, and construction. On the other side, despite the numerous benefits that are offered by social networks to multiple clients worldwide, these social networks address the main requirements for multiple assets to hold a sensible stage of control in real-time. Additionally, in diverse social network settings, the level of trust for the customers should be stated. In the modern era, to fix such major challenges, effective analysis is required to develop enhanced techniques based on the diverse secured and trusted computation, evaluation, and interpretation along with the proper datasets administration of the social networks. Furthermore, there is a mammoth requirement for enhanced techniques to elucidate aspects that relate to secrecy threats to improve present social network secrecy and endorse confidentiality in the social network setting.

However, the privacy of the social network models is very crucial owing to the real-time assaults during the information exchange while the users communicate. Therefore, to resolve all these aforementioned threats, there is a massive requirement to develop a new framework such that the confidentiality and secrecy of the information are maintained over social networks efficiently. In this research, an efficient scheme for the social network model utilizing a dynamic authentication protocol technique has been proposed to maintain the secrecy of information in real-time. Three-Party Authentication Keys Exchange (3PAKE) protocol is recognized as one of the most trusted and important cryptographic techniques which is strongly capable of offering a secured means of communication, thus, allowing two or multiple parties to accord to a fresh secure meeting passcode through the trusted server. Previously, multiple 3PAKE protocols were developed to originate a secured meeting passcode among multiple users as a means of the trusted server. The existing developed 3PAKE algorithms have several limits and are unable to offer the needed confidentiality in social network environments against distinct assaults such as man-in-the-middle, brute force, etc. In this research, first, an enhanced and highly secured 3PAKE technique was developed for social network settings. This 3PAKE protocol is based on a hash function as well as a symmetric encryption technique. The enhanced 3PAKE approach was validated using the well-known AVISPA software. The simulation outcome demonstrates that the proposed 3PAKE protocol is much more secure against diverse active as well as passive assaults like brute-force, man-in-the-middle, parallel assaults, etc. Additionally, the enhanced 3PAKE protocol has a lower processing overhead than existing comparable methods, since it executes very quickly and offers higher levels of authenticity and confidentiality within social network settings. When compared to the earlier methods, this validated 3PAKE approach is found extremely effective and practicable for social network model application in modern communication infrastructure.

To secure the confidential information of users while conversing through any social network, appropriate subscriber authentication is essential. Numerous procedures have been put in place to protect subscribers' private information. However, these techniques contain a variety of flaws to guarantee dataset confidentiality against assaults like cryptanalysis, and man-in-the-middle. Secondly, a modified 3PAKE protocol for social network secrecy is developed in this research which is based on Elliptic Curve

Cryptography (ECC) and Symmetric Encryption (SE). The research findings show how the proposed method takes less duration than conventional procedures and provides the desired security during information exchange over social networks. This enhanced 3PAKE protocol requires 0.09 seconds of search time and communication step 2 which is very minimal during the verification. Moreover, the depth plies were only 3, as well as overall visited nodes were observed at 20. This enhanced 3PAKE technique outcome demonstrates that this modified 3PAKE protocol is an effective method to ensure social network confidentiality during information exchange between the client and authentication server. This proposed 3PAKE protocol offers high-level privacy to the client when communicating over social networks. This technique increases the resilience to numerous recognized assaults, which include replay attacks, and multiple real-time cryptanalysis assaults by numerous attackers. There remain significant possibilities to investigate and integrate new, enhanced procedures for increased security throughout social networks and multiple mobile commerce settings against various active and passive assaults even though numerous researchers conducted comprehensive investigations upon the 3PAKE technique to provide protected data exchange over a social network environment.

## TABLE OF CONTENTS

|   |           |
|---|-----------|
| <b>DECLARATION .....</b>                                      | <b>2</b>  |
| <b>CERTIFICATE .....</b>                                      | <b>3</b>  |
| <b>ACKNOWLEDGEMENT.....</b>                                   | <b>4</b>  |
| <b>ABSTRACT .....</b>   | <b>5</b>  |
| <b>TABLE OF CONTENTS.....</b>                                 | <b>8</b>  |
| <b>LIST OF FIGURES.....</b>                                   | <b>12</b> |
| <b>LIST OF TABLES.....</b>                                    | <b>13</b> |
| <b>LIST OF APPENDICES .....</b>                               | <b>14</b> |
| <b>LIST OF ABBREVIATIONS.....</b>                             | <b>15</b> |
| <b>CHAPTER 1 INTRODUCTION.....</b>                            | <b>16</b> |
| 1.1. Introduction.....  | 16        |
| 1.2. Major elements of social networks .....                  | 16        |
| 1.3. Classification of social networks sites .....            | 17        |
| 1.3.1. Social Connection .....                                | 18        |
| 1.3.2. Multimedia Exchange .....                              | 19        |
| 1.3.3. Professional Social networking sites.....              | 19        |
| 1.3.4. Discussion forums.....                                 | 19        |
| 1.4. Classification of major social networks threats.....     | 20        |
| 1.4.1. Traditional threats .....                              | 20        |
| 1.4.1.1. Spam attack .....                                    | 20        |
| 1.4.1.2. Malware attack .....                                 | 21        |
| 1.4.1.3. Phishing.....  | 21        |
| 1.4.1.4. Identity theft .....                                 | 22        |
| 1.4.2. Modern threats.....                                    | 22        |
| 1.4.2.1. Cross-site scripting assaults.....                   | 23        |
| 1.4.2.2. Profile cloning outbreak.....                        | 23        |
| 1.4.2.3. Clickjacking .....                                   | 23        |
| 1.4.2.4. Hijacking.....                                       | 23        |
| 1.4.2.5. De-anonymization attack .....                        | 23        |
| 1.4.2.6. Cyber espionage .....                                | 24        |
| 1.4.2.7. Inference attack .....                               | 24        |
| 1.4.3. Major Targeted threats .....                           | 24        |
| 1.4.3.1. Cyber-bullying.....                                  | 24        |
| 1.4.3.2. Cyber-stalking .....                                 | 25        |
| 1.4.3.3. Cyber-grooming.....                                  | 25        |
| 1.5. The major cause for social network secrecy threats ..... | 25        |



|  |  |           |
|--|--|-----------|
| 1.5.1.   | Social media scaling.....                                  | 26        |
| 1.5.2.   | Security invisibility.....                                 | 26        |
| 1.5.3.   | Trusted nature.....  | 26        |
| 1.6.   | Pragmatic solutions for diverse threats.....               | 27        |
| 1.6.1.   | Network operator-based solution.....                       | 27        |
| 1.6.1.1.   | Proper Authentication.....                                 | 28        |
| 1.6.1.2.   | Users reporting.....                                       | 28        |
| 1.6.1.3.   | Privacy and secrecy setting.....                           | 28        |
| 1.6.2.   | Academic investigation-rooted solution.....                | 28        |
| 1.6.2.1.   | Phishing detection.....                                    | 29        |
| 1.6.2.2.   | Fake profile identification.....                           | 29        |
| 1.6.2.3.   | Spam identification.....                                   | 29        |
| 1.7.   | Secrecy-related guidelines for social network users.....   | 30        |
| 1.8.   | Different types of generated attack analysis.....          | 31        |
| 1.9.   | Summary.....   | 31        |
| 1.10.  | Thesis layout.....   | 32        |
| <b>CHAPTER 2 BACKGROUND.....</b>   |  | <b>33</b> |
| 2.1.   | Social networks statistics.....                            | 34        |
| 2.2.   | Number of individuals using social networks year-wise..... | 35        |
| 2.3.   | Most penalizing kinds of data breaches.....                | 36        |
| 2.4.   | Main reasons for dataset breach.....                       | 36        |
| 2.5.   | Credential shared by several users.....                    | 37        |
| 2.6.   | Some positive impacts of social networks on users.....     | 38        |
| 2.6.1.   | Social Relation.....                                       | 38        |
| 2.6.2.   | Grouping.....  | 38        |
| 2.6.3.   | Communication.....   | 38        |
| 2.6.4.   | Marketing.....   | 39        |
| 2.7.   | Some negative impacts of social networks on users.....     | 39        |
| 2.7.1.   | Addiction of use.....                                      | 40        |
| 2.7.2.   | Threatening.....   | 40        |
| 2.7.3.   | Secret details exploitation.....                           | 40        |
| 2.7.4.   | Isolation.....   | 41        |
| 2.8.   | Key cybersecurity assaults in social networks.....         | 41        |
| <b>CHAPTER 3 SECURED THREE-PARTY AUTHENTICATION KEY EXCHANGE PROTOCOL.....</b> |  | <b>43</b> |
| 3.1.   | Overview.....  | 43        |
| 3.2.   | Exploration of Social Network Dynamics.....                | 43        |

|   |  |           |
|---|--|-----------|
| 3.3.  | Analysis of Existing Authentication Techniques in Social Networks .....  | 44        |
| 3.4.  | Design Rationale for Dynamic Authentication Protocol.....                | 45        |
| 3.5.  | Implementation Details and Integration Challenges .....                  | 45        |
| 3.6.  | User Experience and Usability Evaluation.....                            | 46        |
| 3.7.  | Performance Metrics and Scalability Assessment .....                     | 47        |
| 3.8.  | Security Considerations in Social Network Authentication .....           | 48        |
| 3.9.  | Application of Dynamic Authentication in Social Networks .....           | 48        |
| 3.10.   | Advancements in Social Network Security with Dynamic Authentication..... | 49        |
| <b>CHAPTER 4 LITERATURE REVIEW .....</b>          |  | <b>51</b> |
| 4.1.  | Review of Chun-Ta-Li 3PAKE protocol .....                                | 57        |
| 4.2.  | Problem Identification .....   | 59        |
| 4.3.  | Objectives .....   | 60        |
| 4.4.  | Research Contributions.....  | 60        |
| <b>CHAPTER 5 PROPOSED WORK (HYPOTHESIS) .....</b> |  | <b>62</b> |
| 5.1.  | AVISPA Software .....  | 62        |
| 5.2.  | Limitations of the AVISPA tool.....                                      | 64        |
| 5.3.  | Advantages of the AVISPA tool .....                                      | 64        |
| 5.4.  | Protocol 1- Enhanced 3PAKE Protocol.....                                 | 65        |
| 5.4.1.  | Notions utilized.....  | 65        |
| 5.4.2.  | Design Enhanced 3PAKE Protocol.....                                      | 66        |
| 5.5.  | Protocol 2- Design .....   | 68        |
| 5.6.  | Protocol 2- System initialization .....                                  | 70        |
| 5.6.1.  | Round 1 .....  | 70        |
| 5.6.2.  | Round 2 .....  | 71        |
| 5.6.3.  | Round 3 .....  | 71        |
| 5.6.4.  | Protocol 2- Safe code exchange stage of enhanced 3PAKE protocol.....     | 72        |
| 5.7.  | Summary .....  | 74        |
| <b>CHAPTER 6 RESULTS AND DISCUSSION.....</b>      |  | <b>75</b> |
| 6.1.  | Protocol 1- Improvised 3PAKE specifications.....                         | 75        |
| 6.2.  | Protocol 1- Improvised 3PAKE secrecy evaluation .....                    | 76        |
| 6.3.  | Protocol 1- Informal secrecy evaluation .....                            | 77        |
| 6.4.  | Protocol 1- Performance computation .....                                | 80        |
| 6.5.  | Protocol 2- Performance analysis .....                                   | 81        |
| 6.5.1.  | Protocol 2- Specifications .....   | 82        |
| 6.5.2.  | Protocol 2- Security evaluation and validation.....                      | 82        |
| 6.5.3.  | Informal security assessment .....                                       | 85        |
| 6.6.  | Simulation results .....   | 88        |

|   |            |
|---|------------|
| 6.7. Summary .....                                      | 91         |
| <b>CHAPTER 7 CONCLUSION AND FUTURE WORK.....</b>        | <b>94</b>  |
| 7.1 Conclusion .....                                    | 94         |
| 7.2. Future Scope.....                                  | 95         |
| <b>APPENDIX A .....</b>                                 | <b>97</b>  |
| 1.1. Enhanced 3PAKE Protocol Specifications .....       | 97         |
| 1.2. Security Analysis of Enhanced 3PAKE Protocol ..... | 97         |
| 1.3. Informal Security Analysis .....                   | 98         |
| <b>APPENDIX B .....</b>                                 | <b>101</b> |
| <b>Bibliography .....</b>                               | <b>104</b> |
| <b>List of Publication.....</b>                         | <b>115</b> |

## LIST OF FIGURES

|  |    |
|--|----|
| Figure 1.1: Illustrates the major elements of social networks. -----   | 17 |
| Figure 1.2: Illustrates the major social network sites. -----  | 18 |
| Figure 1.3: Illustrates classification of social network threats. -----  | 20 |
| Figure 1.4: Illustrates the classification of the traditional threats. -----                                     | 21 |
| Figure 1.5: Illustrates the classification of modern threats. -----  | 22 |
| Figure 1.6: Illustrates the classification of the targeted threats. -----  | 25 |
| Figure 1.7: Illustrates the major cause of social network secrecy threats. -----                                 | 26 |
| Figure 1.8: Illustrates the major threat prevention solutions. -----   | 27 |
| Figure 1.9: Illustrates the major network operator-rooted solutions. -----                                       | 27 |
| Figure 1.10: Illustrates the major network operator-rooted solutions. -----                                      | 29 |
| Figure 1.11: Illustrates the major common secrecy strategies for the users. -----                                | 30 |
| Figure 2.1: Illustrates the global social network statistics. -----  | 34 |
| Figure 2.2: Illustrates the global social network statistics. -----  | 35 |
| Figure 2.3: Illustrates the most penalizing kinds of data breaches. -----  | 36 |
| Figure 2.4: Illustrates the main reasons for datasets breach -----   | 37 |
| Figure 2.5: Illustrates the major positive impacts of social media networking. -----                             | 39 |
| Figure 2.6: Illustrates the major negative impacts of social media networking. -----                             | 40 |
| Figure 2.7: Illustrates the major key cybersecurity assaults in social networks. -----                           | 42 |
| Figure 5.1: Depicts the interface of the AVISPA software. -----  | 62 |
| Figure 5.2: Depicts the 3PAKE protocol verification summary on 10 nodes. -----                                   | 63 |
| Figure 5.3: Depicts the 3PAKE protocol verification summary on 20 nodes. -----                                   | 63 |
| Figure 5.4: Depicts flow chart of hash function and symmetric encryption based on improved 3PAKE protocol. ----- | 68 |
| Figure 5.5: Illustrates the first round of the improvised 3PAKE protocol. -----                                  | 71 |
| Figure 5.6: Illustrates the second round of the improvised 3PAKE protocol. -----                                 | 71 |
| Figure 5.7: Illustrates the third round of the improvised 3PAKE protocol. -----                                  | 72 |
| Figure 6.1: Depicts authentic main server $S_a$ role for verification. -----                                     | 78 |
| Figure 6.2: Depicts session role for verification of enhanced 3PAKE. -----                                       | 78 |
| Figure 6.3: Depicts environmental role for verification of enhanced 3PAKE. -----                                 | 79 |
| Figure 6.4: Depicts analysis goal for verification of enhanced 3PAKE. -----                                      | 79 |
| Figure 6.5: Depicts simulated results through the OFMC back-ends. -----  | 81 |
| Figure 6.6: Depicts stated role for authentic main client CLA. -----   | 83 |
| Figure 6.7: Depicts stated role for authentic main client CLB. -----   | 84 |
| Figure 6.8: Depicts the stated role of authentic main server SRA. -----  | 85 |
| Figure 6.9: Depicts the main role of the session. -----  | 86 |
| Figure 6.10: Depicts the main role of the environment. -----   | 86 |
| Figure 6.11: Depicts the main role goal of improvised 3PAKE. -----   | 87 |
| Figure 6.12: Depicts the simulated outcomes through the OFMC back-end. -----                                     | 87 |
| Figure 6.13: Depicts the enhanced 3PAKE protocol execution time. -----   | 89 |
| Figure 6.14: Depicts enhanced 3PAKE protocol communication step and visiting node comparison. -----              | 90 |

## LIST OF TABLES

|  |    |
|--|----|
| Table 2.1: Illustrates the datasets of individuals. ....   | 37 |
| Table 4.1: Illustrates the existing state-of-the-art techniques used for security verification and their drawbacks. .... | 55 |
| Table 5.1: Illustrates the notations used and their definitions. ....  | 66 |
| Table 5.2: Shows abbreviations used in improvised 3PAKE protocol. ....   | 69 |
| Table 6.1: Illustrates the symbols used in the Sa role. ....   | 76 |
| Table 6.2: Depicts enhanced 3PAKE protocol results for the social networking model. ....                                 | 81 |
| Table 6.3: Illustrates chosen symbols in multiple roles of improvised 3PAKE. ....  | 82 |
| Table 6.4: Shows a comparative analysis of the results of improvised 3PAKE. ....   | 88 |

# **LIST OF APPENDICES**

APPENDIX A

**Enhanced 3PAKE Protocol Specifications**

**Security Analysis of Enhanced 3PAKE Protocol**

**Informal Security Analysis**

APPENDIX B

## LIST OF ABBREVIATIONS

|        |  |
|--------|--|
| 3PAKE  | : Third Party Authenticated Key Exchange                               |
| HF     | : Hash Function  |
| SE     | : Symmetric Encryption   |
| ECC    | : Elliptic Curved Cryptography   |
| OSN    | : Online social networks   |
| IT     | : Information Technology   |
| XOR    | : Exclusive OR   |
| OTP    | : One Time Password  |
| KCI    | : Keys compromise impersonation  |
| DHKE   | : Diffie-Hellman Key Exchange  |
| AVISPA | : Automated Validation of Internet Security Protocols and Applications |
| HLPSL  | : Higher-Level Protocols-Specific Languages                            |
| SNS    | : Simple Notification Service  |

# CHAPTER 1 INTRODUCTION

## 1.1. Introduction

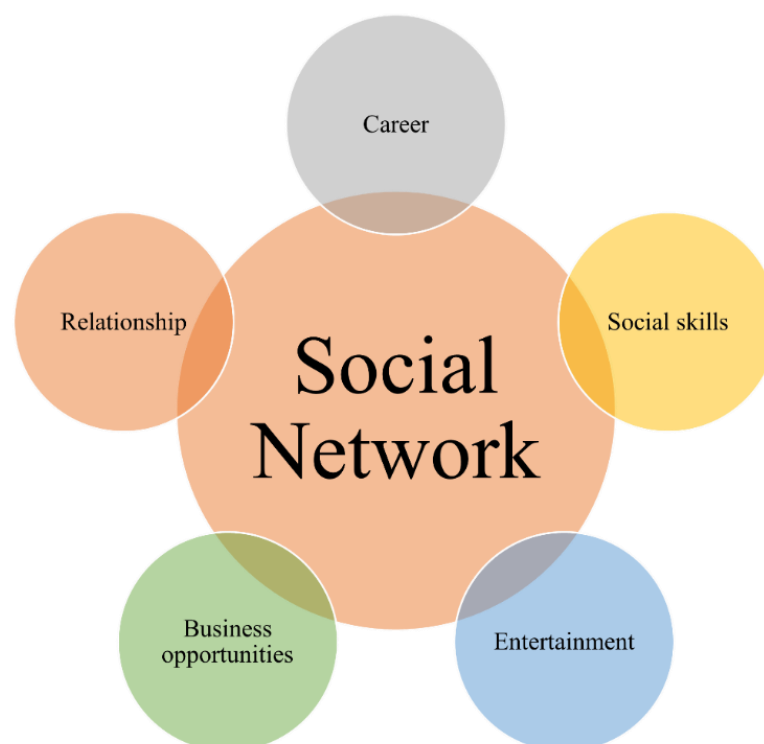
The secrecy and privacy of social networks have become a very serious and challenging threat all around the globe in recent years. Social networks provide a means to multiple users for information exchange worldwide. However, these social networks have distinct vulnerabilities related to information secrecy as well as privacy, which demand more attention towards pragmatic solutions to maintain data secrecy during information exchange over the networks. In simple terms, social networks are pragmatic social platforms built by a group of social actors (for instance, the organization, individual, etc.), grouping, and multifarious social communication amongst the actors. Furthermore, the social network viewpoint offers a group of techniques to analyze the overall social entity construction along with diverse theories that explain detected patterns within these architectures [1]. A thorough study of such architectures utilizes social network evaluation to identify global and local patterns, along with the network dynamics evaluation. The necessity of low-power smartphone gadgets and secured transmission between these gadgets is growing rapidly due to the enormous rise of information and telecommunication technologies (ICT). Numerous confidentiality concerns have been highlighted amongst customers utilizing cellular gadgets and service operators via the Internet. Insecure networks elevate the likelihood of illegal accessibility, data tampering, stealing, and direct harm to objects holding highly private data. To protect communication networks from various assaults information security is a top priority, thereby novel communication protocols need to be investigated [2], [3].

## 1.2. Major elements of social networks

In recent years, online social networks (OSNs) have experienced an extraordinary rise in popularity, fuelled by the rapid progression of technological innovations. These OSNs offer a venue for people to communicate with relatives, neighbors, and co-workers. Social networks provide effective means of communication through various mediums such as text messaging, and image exchange, thereby aiding



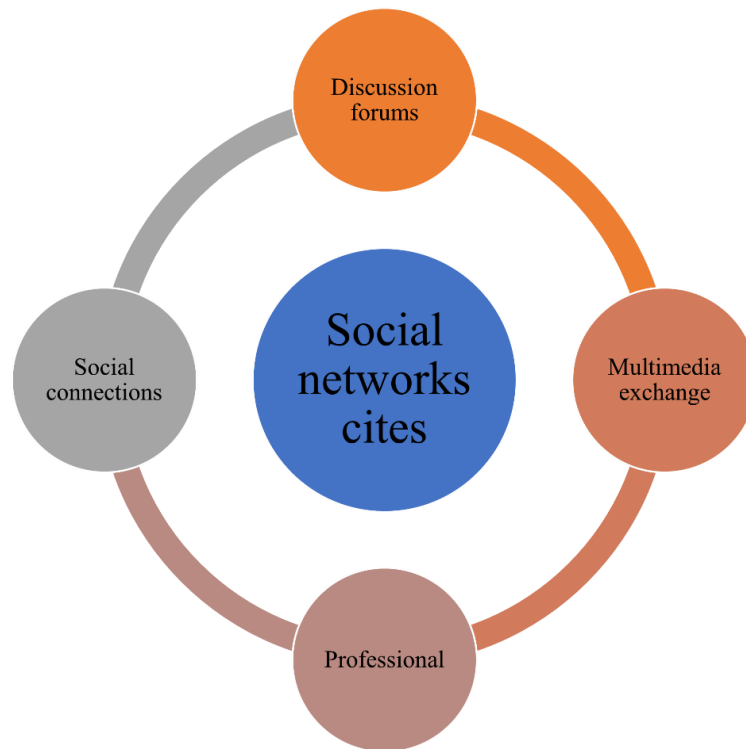
in rapid information exchange among users. The confidentiality of the OSNs must be investigated from a variety of angles. The recipient's sharing of information raises safety and confidentiality concerns, particularly whenever an individual translates private stuff like images, video recordings, etc. Shared data can be cracked by the hacker by using distinct methods during the communication process [4], [5]. Whenever youngsters are targeted by hackers, then hazards are significantly greater. Figure 1.1 illustrates the major elements of social networks. The major OSN elements include entertainment, business opportunities as well as social skills including career-long relationships.



**Figure 1.1: Illustrates the major elements of social networks.**

### **1.3. Classification of social networks sites**

Social networks may be categorized into several classes according to specific purposes. The four basic categories of social networks are classified as social connection, exchange of multimedia, professionals, and discussion forums. Various sorts of social network websites and their susceptibility, including incidents of spoofing have taken place in distinct classes. Furthermore, multiple ongoing issues of social networks have been identified, with a focus on harmful content-based phishing assaults [6]. Figure 1.2 illustrates the classification of social network sites.



**Figure 1.2: Illustrates the major social network sites.**

### 1.3.1. Social Connection

Social networks are used by various users to interact virtually with businesses and other users. Even though there exist multifarious online public network websites around the world, however, information privacy is a very challenging task in real-time user interaction. These websites can be classified as follows: LinkedIn, Instagram, Facebook, as well as Myspace, and many more. Such websites offer ease in the communication process, but there exist numerous drawbacks related to data breaches. These websites are susceptible to spoofing and malware assaults in a variety of manners. The gateway appears like a Facebook account might be created by an intrusive party or user. The users can input personal information to register on social network websites very quickly [7]. The vital social connection insights are described as follows:

- Transmitting counterfeit posts that describe regarding individual Facebook account may be inactivated.
- Any user might be misled into opening a phishing URL (Uniform Resource Locators) inside a personalized post from such a buddy that claims the person's private photos have been published there.

- Several hackers say that the users' profile has to be upgraded to continue using them in their messages. A downloading URL of the upgrade is provided, which includes the URL of the fraudulent website.

### **1.3.2. Multimedia Exchange**

The social network for information exchange content is employed to upload and distribute digital images, recordings, streaming videos, etc. Social networks provide an effective means for consumers and corporate organizations to exchange and publish digital content. These social websites include YouTube, Flickr, Twitter, as well as Snapchat, etc. Currently, the modern networking platform includes an inbox function wherein users can mail and communicate with personal contacts. Furthermore, YouTube is the most effective and widespread medium utilized by the masses for multimedia content exchange. The hacker has various options to break the communication using distinct methods and is capable of phishing the victims. The attacker may include a truncated URL in the text that takes the reader's attention to the phishing spot. Intruders benefit from the fact that it's difficult to tell if a truncated URL seems valid or not, thereby concealing any harmful material in truncated URLs.

### **1.3.3. Professional Social networking sites**

Commercial social networks have been created to present individuals with employment prospects. According to the site's purpose, this could offer a public platform or be targeted at certain interests or professions. Corporate social network platforms include LinkedIn, Classroom 2.0, Pinterest, and many more. Because the recipient's official data, especially their contact address is stored on such virtual network's websites, a hacker could use this data to deliver a target customized message. Such messages could resemble emails offering prizes and include a harmful hyperlink [8].

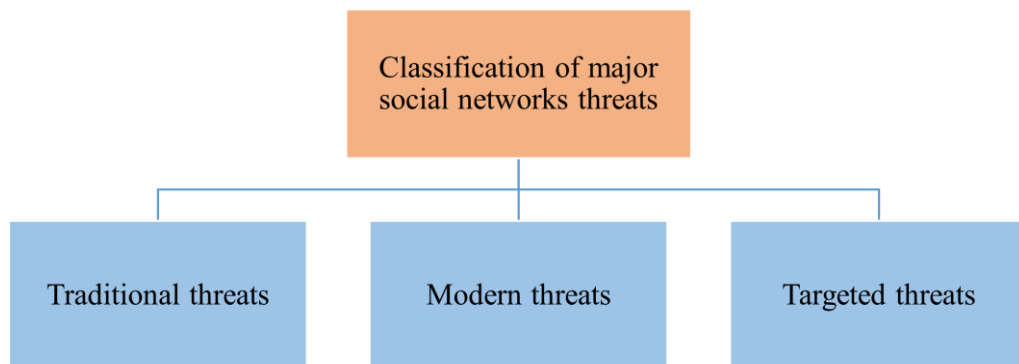
### **1.3.4. Discussion forums**

Individuals also utilize social platforms to debate subjects and exchange ideas within conversation groups. These discussion forums are classes of interpersonal networks and optimal tools for marketplace study. Prominent debate platforms include Reddit, Quora, Digg, and many more. Users can also post connections to personal study in such areas such that other individuals may learn further regarding the subject of their study. Many times, harmful hyperlinks are distributed by certain unauthorized

individuals to direct visitors to fake web pages. Hacking may also be carried out similarly on online platforms [9].

#### 1.4. Classification of major social networks threats

People have expanded their engagement with this digital sphere of the web since they live in a technologically advanced culture even though it is very widespread. Various assaults that people have encountered since social networks first started are listed beneath. These major threats have been split under three classifications i.e., the traditional threats, and modern threats, including the main targeted threats [10]. Figure 1.3 illustrates the classification of social network threats.



**Figure 1.3: Illustrates classification of social network threats.**

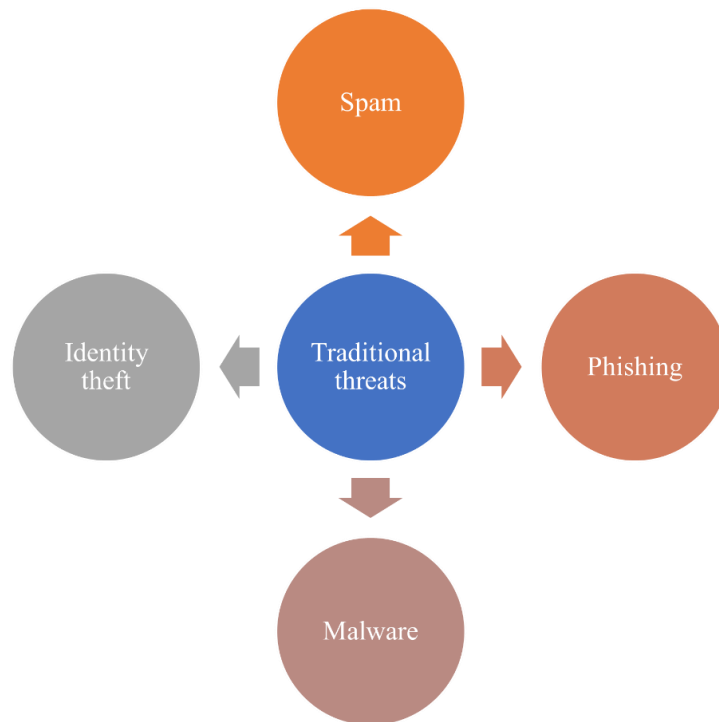
##### 1.4.1. Traditional threats

These kinds of threats are a diverse category of threats in which individuals experience issues from social network initial development. Such kinds of threats are crucial to handle large detection and handling time, along with large computation costs in real-time. The traditional threats further may be categorized into multiple classes as described in Figure 1.4.

###### 1.4.1.1. Spam attack

Unrequested mass computerized emails are known as spam. Even though email is a typical means of transmitting junk, social networking sites are increasingly effective. Through corporate portals, forums, and newsgroups, it is simple to get the correspondence information of genuine customers. It's simple to mislead the intended customer to accept spam emails and assure the user about the information security. While the majority of spam messages are typically promotional adverts, however, some

of them might include worms, spyware, or frauds which might be utilized to harvest consumers' data [11].



**Figure 1.4: Illustrates the classification of the traditional threats.**

#### **1.4.1.2. Malware attack**

Malware includes harmful software that has been specifically developed to infect or gain entry within a computing machine, typically beyond the individual's consent. A hacker has a wide range of options for contaminating networks and gadgets with the virus. For example, any hostile URL could direct a user to a fake website that tries to collect personal information about them to download spyware inside the system. Any intruder could include harmful programs into URLs, therefore if a user clicks on the URLs, malware runs on the target machine and potentially gathers valuable data through it. These viruses leverage underlying online social networking architecture, including the number of nodes, connections, median lowest route, and largest pathways, across various connecting sites to spread themselves [12].

#### **1.4.1.3. Phishing**

This phishing assault is a type of socially engineered assault wherein the attacker obtains private data from the victim, such as login, passcode, and credit card data, by using counterfeit webpages including emails that look to be authentic. Any hacker might assume the identification of a legitimate individual and utilize this to

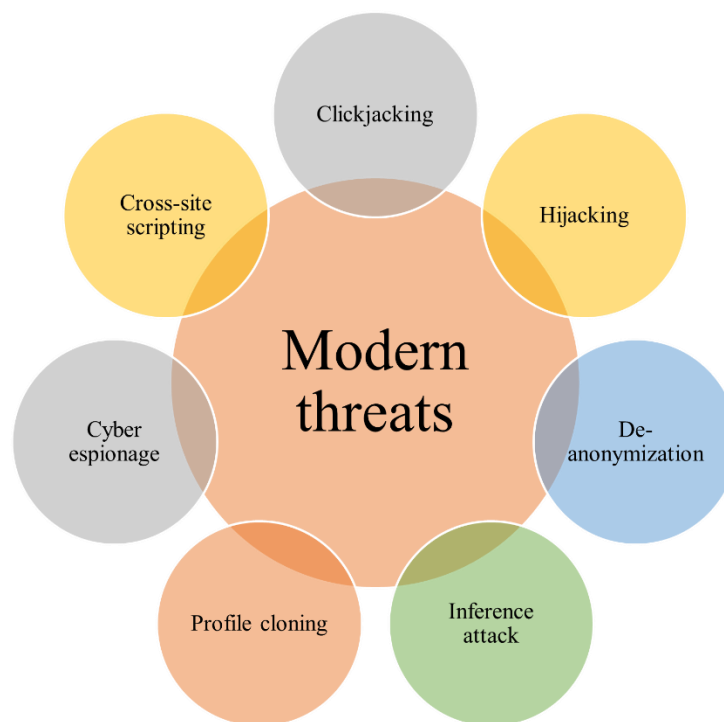
transmit false messaging to another individual through a social media site that includes hazardous URLs. These URLs could reroute a user toward the fake webpage wherein sensitive details are requested. In the context of SNS (Simple Notification Service), any attacker must entice the victim to a fake website so that he may launch a hacking attempt [13].

#### 1.4.1.4. Identity theft

In an identity hack, an online intruder gets another person's credentials, including personal social identification information, cell phone number, and location, despite that person's consent. The hacker may quickly acquire a victim's buddy directory with the use of such credentials and obtain confidential data from individuals utilizing various socially engineered tactics. The intruder may access the account in whatsoever manner the attacker sees fit because the attacker is posing as a valid customer, which might hurt real customers [14].

#### 1.4.2. Modern threats

This is another advanced category of assaults that are utilized by the attacker to get confidential datasets of the users in real-time. The modern threat further can also be categorized into diverse classes as depicted in Figure 1.5.



**Figure 1.5: Illustrates the classification of modern threats.**

#### **1.4.2.1. Cross-site scripting assaults**

Cross-site scripting seems to be a highly common assault tactic used by hackers. This assault is referred to simply as "Self-XSS" and shortened to just XSS. Primarily, the assault employs a variety of methods to install dangerous JQuery just on the user's computer. These assaults have been categorized among DOM-rooted, persistent, and reflected-XSS assaults. With only one press of any link, the computer might be taken over, potentially sending a dangerous program into a computer [15].

#### **1.4.2.2. Profile cloning outbreak**

In such an approach, the attacker copies the victims' profiles that he is already familiar with. The hacker may establish a trustworthy association with the followers of the genuine person using a such replicated profile on an identical and a different socially connecting portal. When one link has been made, the assailant manipulates the suspect's associates into accepting the legitimacy of the counterfeit resume and, therefore, can effectively get confidential data that is typically not revealed within their accessible resumes. Cyberbullying, as well as cyber stalking along with cyber extortion, are further forms of cyberattacks that could be committed using such assaults [16].

#### **1.4.2.3. Clickjacking**

Throughout the process of clickjacking, an online client is tricked into clicking on a website other than the one individual meant to visit. This has been often referred to as an assault on the client's appearance. The hacker carries out such assault by taking advantage of the computers' vulnerabilities [17].

#### **1.4.2.4. Hijacking**

When a person's profile is hijacked, the opponent breaches or seizes access to commit digital scams. Since credentials may be stolen via hacking, websites lacking multifactor authorization and profiles having poor credentials are highly susceptible to takeover. Without multifactor identification, users don't possess a backup point of protection. When a profile has been taken over, the hacker can compose emails, distribute harmful links, and modify profile details, all of which might destroy the person's identity [18].

#### **1.4.2.5. De-anonymization attack**

Individuals may utilize an alternative or made-up username on several social networking platforms, including Twitter, and Instagram, to safeguard actual true

identities without disclosing personal information. However, any third party may easily determine the person's genuine identity by correlating the data exposed through such online social platforms. To determine customers' true identification, they employ techniques including monitoring cookies, networking protocols, and user account membership [19].

#### **1.4.2.6. Cyber espionage**

Cyber espionage is the practice of gathering confidential data or intellectual assets online to pass the same along to adversaries. An unauthentic user tries to access the intellectual property for political gain as well as competitive advantage. Such assaults are frequently utilized as a component of combat operations as a means of criminal extortion and driven by a desire to seek financial gain.

#### **1.4.2.7. Inference attack**

Considering the multifarious insights that the customer posts on SNS the inferred assault could be employed to deduce an instructor's confidential data that this same client could not wish to expose. On accessible information, such as the person's buddy group and networking architecture, it employs dataset mining techniques. An assailant could discover a company's confidential data or a person's location and technical background by utilizing such an approach [20].

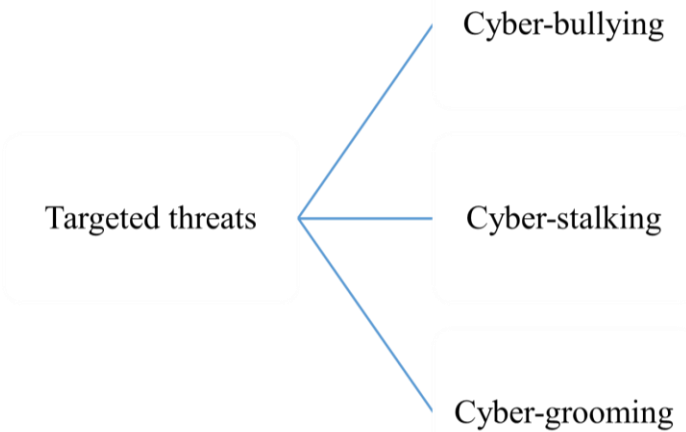
### **1.4.3. Major Targeted threats**

Assaults that are directed towards a specific individual could be carried out through any one individual for a variety of individual grudges. These kinds of major targeted threats can be categorized into the following diverse three separate classes as depicted in Figure 1.6.

#### **1.4.3.1. Cyber-bullying**

Cyber-bullying occurs when someone is bullied or harassed via digital communication tools including messages, chatting rooms, cell phone calls, and digital networking sites. Cyberbullying is a continual procedure, in contrast to conventional harassment. Social networks are used to regularly manage content. To stalk any individual, the assailant frequently delivers threatening texts, and videos to promote rumors, and occasionally releases humiliating images or movies [20], [21].





**Figure 1.6: Illustrates the classification of the targeted threats.**

#### **1.4.3.2. Cyber-stalking**

Cyber-stalking is indeed the act of following someone online, via emails, or via any kind of digital contact which makes someone fear for their safety and disturbs their psychological tranquillity. An individual's claim to anonymity is violated. The assailant keeps a record of the targets' private or confidential data and utilizes this to continuously as well as persistently harass individuals all day long. Such behaviors incite a form of worry, anxiety, or agitation inside the sufferer which causes them to be extremely concerned about their security [22], [23].

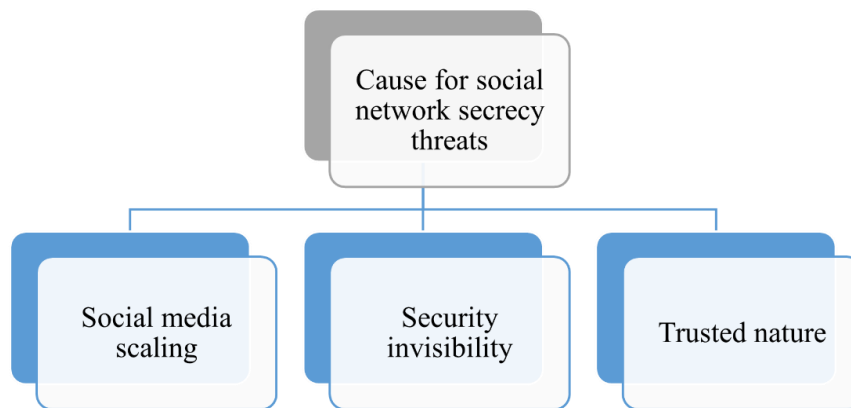
#### **1.4.3.3. Cyber-grooming**

Forming a close, empathetic bond with online victims, typically youngsters and teenagers, to coerce sexual assault is known as cyber grooming. One main goal behind cyber grooming would be to win over children's confidence so that more personal, and sensitive data, may be obtained about them. Information from explicit discussions, images, and movies is frequently sensuous in tone, giving the assailant the personal benefit of threatening and blackmailing the users [24], [25].

### **1.5. The major cause for social network secrecy threats**

Throughout this modern era, social networking handles a number of the biggest singular, and uncontrolled information, but such a scenario is spreading swiftly everywhere. Millions of users post personal images and various multimedia information each day on online networking sites so that their connections may view them [26]–[28]. This creation of computerized hazard assessment is being prompted in the modern world. Additional safety requirements that place customers

(representatives, customers, and associates) squarely inside the direct range of an attacker have been introduced by the growth of web-rooted media. Assailants now view online networking as a potential online high point in which it is easy to approach individuals. Among the largest and greatest potent threats to authority, safety has been provided by it. Assailants use online networking for these diverse three causes listed below [29], [30]. Figure 1.7 illustrates the major cause of social network secrecy threats.



**Figure 1.7: Illustrates the major cause of social network secrecy threats.**

#### **1.5.1. Social media scaling**

Because such a large number of individuals use online networking for a variety of reasons, assaults could become global just like anything new movement. The offender could promote their virus, which may be targeted at everybody or just a certain group of people, using keywords, sensationalism, including controversial subjects. Technically overcoming these creates a huge difficulty for safety professionals [31], [32].

#### **1.5.2. Security invisibility**

Social media platforms are where the bulk of individuals around the globe devote this bulk of their leisure. Because safety personnel lack the capabilities to expand overall detectability outside a certain boundary into the digital networking realm, wherein personnel is especially susceptible to penetration, watching such a vast population becomes incredibly difficult [33]–[35].

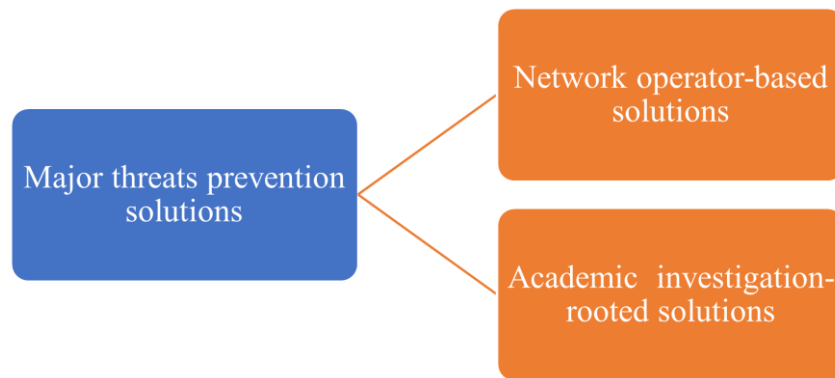
#### **1.5.3. Trusted nature**

The trustworthy character of social networking sites is hacked by attackers. The premise of common connections, the recipient possesses, individuals will occasionally approve an unfamiliar person's invite. Despite giving any thought to a potential safety

violation, people quickly click on the hyperlink shared by other colleagues. Internet content may be the finest way to get user insights because more than one-third of such individuals use social networks and accept invites from strangers [36], [37].

### 1.6. Pragmatic solutions for diverse threats

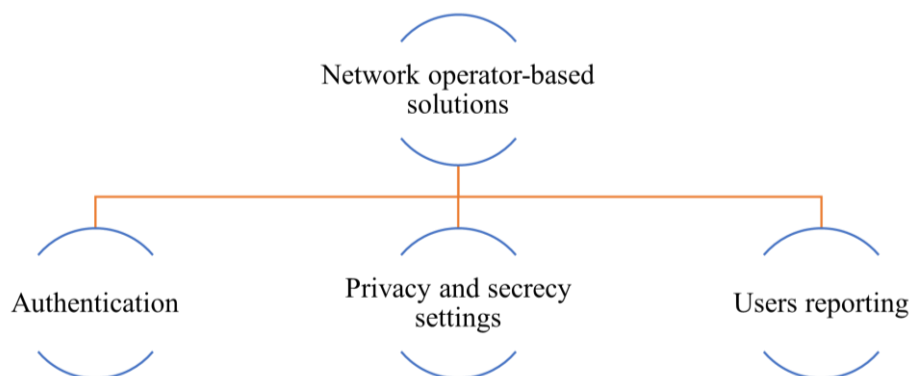
Numerous experts from both academics and businesses are working nonstop to develop answers to the abovementioned modern networking risks. Researchers have put out several ideas including strategies to counter such dangers. There is discussed numerous techniques and strategies for SNS safety that have been utilized by numerous academics. These approaches have been divided into two categories: namely social networking providers and educational institutions [38], [39]. Figure 1.8 illustrates the major threat prevention solutions.



**Figure 1.8: Illustrates the major threat prevention solutions.**

#### 1.6.1. Network operator-based solution

Network operator-based solutions are very essential and play a crucial role in securing the confidential datasets of the individual more pragmatically. These kinds of solutions may be categorized as illustrated in Figure 1.9.



**Figure 1.9: Illustrates the major network operator-rooted solutions.**

#### **1.6.1.1. Proper Authentication**

Numerous online social networks utilize verification processes like CAPTCHA, and multi-factor verification, including identification of friend photographs to ensure that a real person is entering inside and trying to join the social network. For example, two-factor verification is used by popular public networking such as Facebook and LinkedIn [40]–[42]. Such an idea makes utilization of a smartphone device-delivered passcode and registration passcode. It decreases the chance that any username will be hacked, thus stopping an intruder from stealing a genuine password but also using the same to publish bad stuff [43].

#### **1.6.1.2. Users reporting**

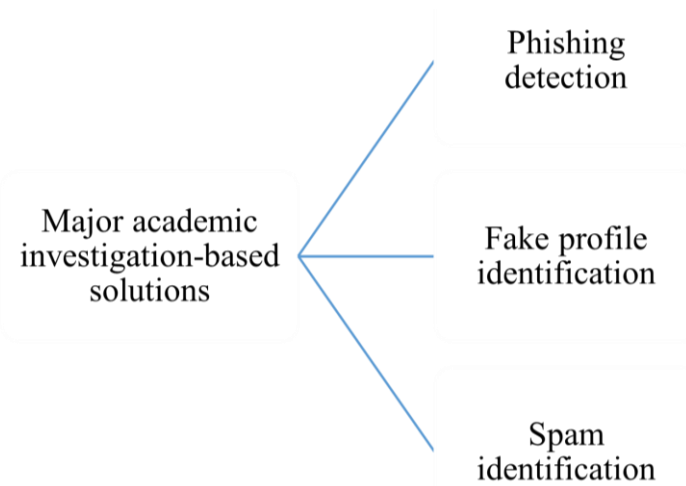
Digital platforms safeguard the next generations especially minors against harassment by enabling users to notify unwanted misconduct or rules breaches through other users. For illustration, a person may employ the complaint hyperlinks to deliver a direct email to any person who published anything to Instagram requesting someone to delete anything when it offends their sensibilities but does not break Instagram's rules of conduct. Following an assessment and removal of the following Instagram group guidelines, complaints are received by Instagram [44].

#### **1.6.1.3. Privacy and secrecy setting**

Several social connecting websites include dependable safety and confidentiality settings so that users may protect their sensitive data against unauthorized accessibility through third parties or programs. For example, any Instagram customer allows users to change personal privacy settings but also chooses which users within the community (associates, buddies who are friends, as well as everyone) may access personal profile data, photos, messages, and additional critical data. Instagram also gives individuals the option of accepting or rejecting the accessibility of outside programs to sensitive data. Various socially connecting websites have inner system public safety features installed. These protect networking participants from junk mail, fake products, fraudsters, and other hazards [45]–[47].

#### **1.6.2. Academic investigation-rooted solution**

The academic study-based solutions provide a means for identifying diverse secrecy-related threats to the user's confidential information transmitted with the help of online social networks. These kinds of diverse solutions can be categorized into the following classes as depicted in Figure 1.10.



**Figure 1.10: Illustrates the major network operator-rooted solutions.**

### **1.6.2.1. Phishing detection**

Numerous conventional online applications, including webpages, social network platforms, messages, including forums, are compromised by hacking in terms of confidentiality as well as integrity. To identify fraudulent assaults, numerous averse-phishing strategies have indeed been created. Numerous experts have already proposed averse-phishing practices depending on methods meant to recognize spoofing webpages including URLs. The academic world has proposed specific remedies for scamming assaults inside a socially connecting setting as phishing assaults increasingly get greater prevalent on digital connecting platforms [48].

### **1.6.2.2. Fake profile identification**

One method for identifying fake profiles as well as products is described by the researcher in Reference [49]. Researchers took certain user-generated information through the LinkedIn website and analyzed it to retrieve various attributes. Following the main constituent pre-processing of individual profiles. Further, a neural network-based robust backpropagation method has been used to build a trained dataset.

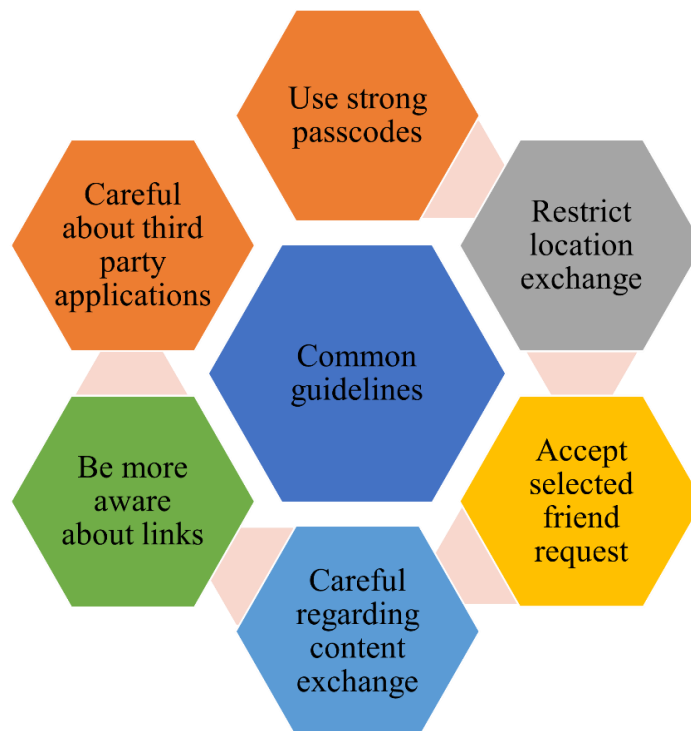
### **1.6.2.3. Spam identification**

To address the problem of spamming attacks on Instagram, Rathore et al. introduced another Spam Spotter architecture. This smart choice supporting platform serves as its foundation. Through these same usages of the proposed choice supporting system, this collects pertinent data from the customer account and afterward evaluates this by tying the customer dataset to the categorization of a customer account as either authentic or spammy. This addresses many of these problems as well as difficulties. (a)

This addresses the problem of the overall majority of spamming identification systems' insufficient array of characteristics. (b) This addresses these same issues of open accessibility and ambiguity around important Instagram data. (c) Lower accuracy and long reaction times are resolved by using this technology. To identify Instagram spamming, machine learning models within the proposed application offer quick reaction times [50].

### 1.7. Secrecy-related guidelines for social network users

Online community networks and media are becoming an essential aspect of everybody's lives. The dangers of utilizing such online media platforms increase along with their notoriety. Each year, this quantity of subscribers grows significantly. Therefore, protecting customers on such sites remains essential. People may follow the safety recommendations listed below to maintain themselves relatively secure [51], [52]. In social networks different platform such as Twitter, Facebook, blogs, wikis, etc. allows people to interact with each other. Certain common guidelines, such as using strong passcodes, restricting location exchange, being cautious about third-party applications, being more aware of links, accepting selected friend requests, and being cautious about content exchange, require different approaches. Figure 1.11 illustrates the major common secrecy strategies for the users.



**Figure 1.11: Illustrates the major common secrecy strategies for the users.**

## **1.8. Different types of generated attack analysis**

This work is focused on addressing multifarious assaults widespread in social networking such as brute-force, parallel attacks, as well as man-in-the-middle, etc. Such assaults pose huge problems to the integrity and secrecy of communication channels inside social networking, requiring robust secrecy measures to eliminate their impact. By leveraging the symmetric encryption and hash function combination, this suggested 3PAKE algorithm was developed to establish a secured communication link and strengthen defense against distinct assaults in real-time, thereby ensuring a secured communication connection amongst users. Starting through the recognition as well as defining distinct assault scenarios related to the 3PAKE algorithm and social networking settings. There are considered common assaults for secrecy verification such as brute-force assaults, replay as well as parallel assaults, etc. Moreover, the attack scripts were developed to simulate the recognized assault settings. The script was tailored to particular threats as well as weaknesses inherent in the suggested 3PAKE algorithm implementation. For instance, in man-in-the-middle, replay, and brute-force assaults, the developed script intercepts and customizes the messages interchanged amongst the parties to mimic authentic users. There are used AVISPA software for secrecy verification of suggested methods that authorize against passive as well as active assaults. Particularly, the research outcome of the 3PAKE protocol implementation shows the performance against man-in-the-middle, brute-force, parallel assaults, and many more.

## **1.9. Summary**

The research work carried out in this thesis focussed on enhancing social network secrecy by implementing the new 3PAKE algorithm. This enhanced 3PAKE algorithm is based on a hash function and symmetric encryption. The key reason to investigate this algorithm was to address the threats of existing protocols developed for providing secrecy to the confidential information, thus offering additional secrecy to the user against distinct assaults namely cryptanalysis, replay assaults, man-in-the-middle, as well as brute-force. This chapter summarizes the classification of social networks and key threats, major causes for social network secrecy threats, pragmatic solutions for distinct threats, secrecy-related guidelines for social network users, and distinct kinds of generated assaults analysis.

### **1.10. Thesis layout**

This thesis layout is described as follows: Major elements of social networks and their classification, key social network threats, key solutions, and secrecy-related guidelines for social network users are described in Chapter 1. Furthermore, the background information on social network statistics, most penalizing kinds of data breaches, positive and negative impacts of social networks on users, and key cybersecurity assaults in social networks are covered in Chapter 2. Moreover, the secured three-party authentication key exchange protocol is explained in Chapter 3. Previous research carried out on the 3PAKE protocol has been given in Chapter 4. In addition to this, details of the proposed research work have been explained in Chapter 5. Specifications of improvised 3PAKE protocol, informal secrecy evaluation, and simulation results are discussed in Chapter 6. Lastly, the future scope of the conducted research is explained in Chapter 7.



## CHAPTER 2 BACKGROUND

Data could now be shared using multifarious methods that had never been conceivable previously whenever the web first gained popularity throughout the middle of the 1990s. However, the exchange of data over communication channels yet lacks a human touch. Later, online social websites introduced a personalized preference to electronic data exchange throughout the mid-2000s, that was well-associated by the masses. This process of social networks involves establishing new connections with people, usually via digital networking platforms such as LinkedIn, Instagram, as well as Snapchat, etc. It may be utilized for equally private and professional purposes. Individuals come together because of this to converse, exchange views, learn skills, and even meet lifelong friends [53]. In essence, this fosters communication among individuals across various regional locations. Websites for virtual socializing have indeed been widely regarded as highly user-friendly.

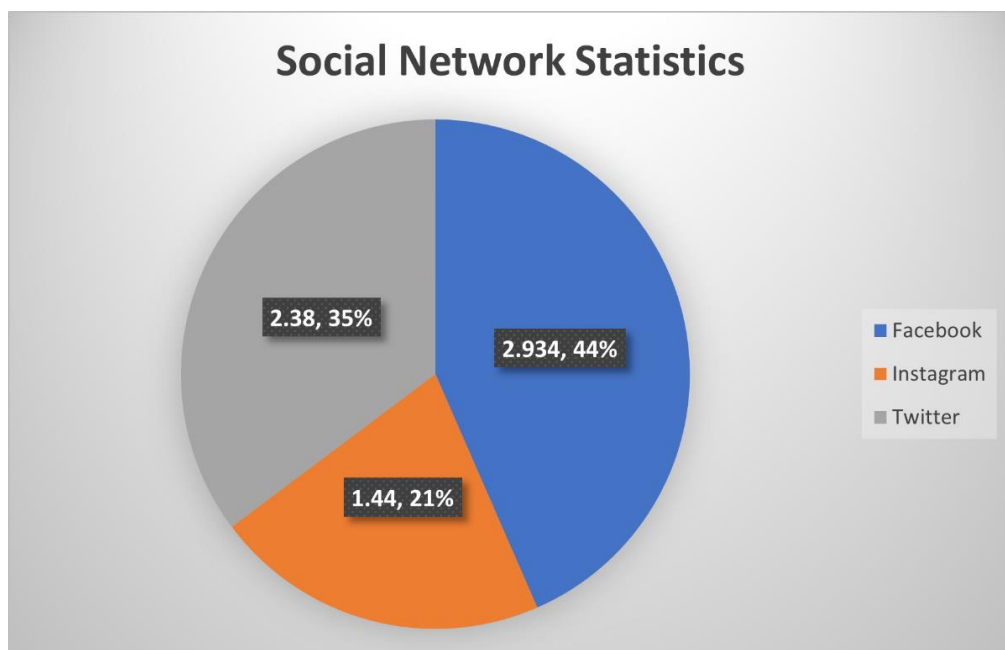
Digital network platforms are becoming significantly greater prominent and numerous for such purposes. Social networks may be utilized for fun, generating commercial possibilities, launching a trade, enhancing interpersonal abilities, including establishing connections with similar people. A couple of the biggest popular professional social websites include Facebook and Instagram. Facebook networking has already grown to be a very important tool for promoting businesses and outreach campaigns because a considerable portion of the internet populace uses it. Individuals frequently take into account this same significance of protecting the data they keep on socially connecting websites because they view them as particular interaction tools. Individuals are gradually posting bigger and bigger data over virtual platforms inside a variety of formats, which might result in unparalleled accessibility to personal as well as corporate data. Social networking users retain a lot of data, making it particularly tempting for opponents looking to cause damage [54]–[56]. With such an enormous quantity of knowledge at their disposal, hackers might unleash global damage. Additionally, digital networking has developed into a fantastic platform for marketing, because if manufacturers do not treat online network privacy concerns sufficiently, they

expose business confidential information to danger as well as leave themselves up to a range of risks [53], [57].

To resolve such problems, this thesis offers a detailed analysis of the many cybersecurity and confidentiality dangers as well as available approaches that could offer social media networking subscribers protection. Through mentioning specific statistical data, it has indeed examined the online social networking site's assaults on numerous online social networking apps. Additionally, there have indeed been spoken about a lot of preventive measures for social network safety. Ultimately, this research thesis analyses unresolved problems, difficulties, and pertinent safety recommendations for building trust within digital socializing networking.

### 2.1. Social networks statistics

The utilization of social networks has increased continuously owing to multiple factors such as more internet accessibility with greater speed globally, more availability of smartphones particularly in developing nations, and many more. Presently, there are approximately more than 4.48 billion individuals who are actively utilizing diverse social media platforms namely Facebook as well as Instagram Twitter, and several others [58]–[60].



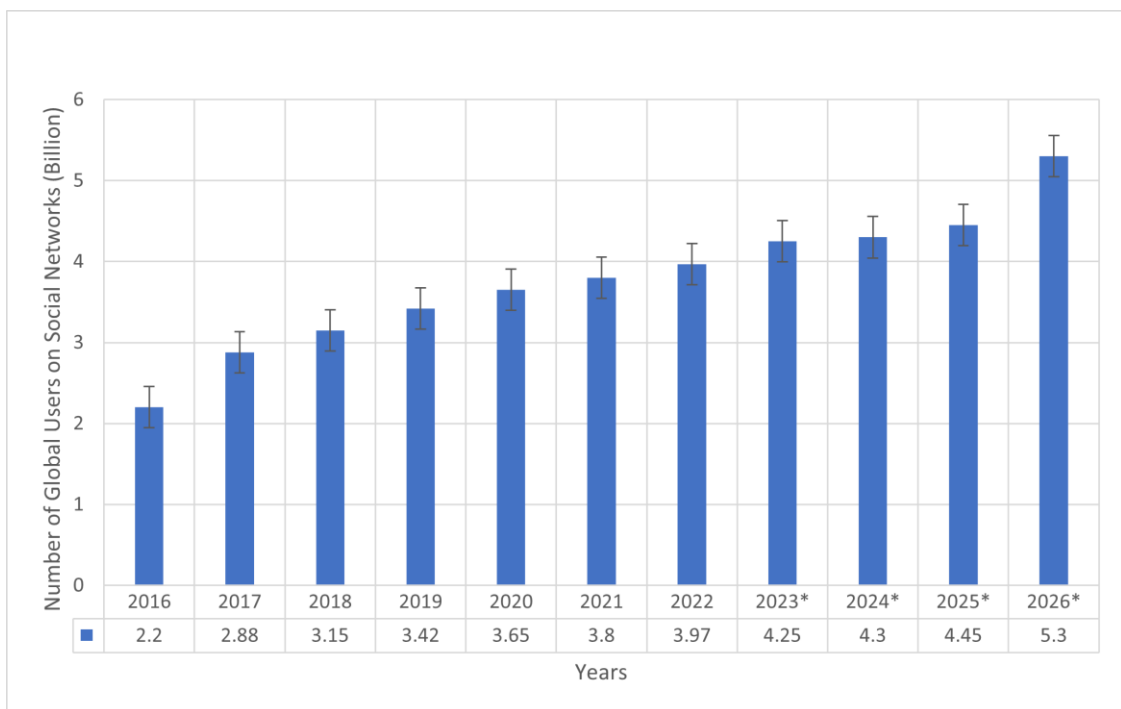
**Figure 2.1: Illustrates the global social network statistics.**

As per the reports, there are approximately 2.9340 billion individuals who are actively using Facebook for diverse purposes. There are approximately 1.4400 billion

active individuals worldwide on the Instagram platform who are utilizing Instagram in day to day lives for sharing images, chatting, and many other purposes. Furthermore, another report states that there are approximately 2.380 million active individuals on Twitter [61], [62]. Figure 2.1 illustrates the global social network statistics.

## 2.2. Number of individuals using social networks year-wise

According to the statistics of the relevant dataset shown in Figure 2.2, this utilization of social media platforms has grown rapidly, resulting in a huge quantity of datasets and details accessible on both such webpages. This has indeed elevated the danger of dataset leaching and created opportunities for many such dataset breaches, including dataset interception, confidentiality snooping, copyright violation, as well as other datasets forgery. Even though certain virtual network websites, including Facebook, forbid members from sharing personal data, certain skilled hackers may deduce confidential details by scrutinizing individual postings, and data of individuals may be provided publicly.



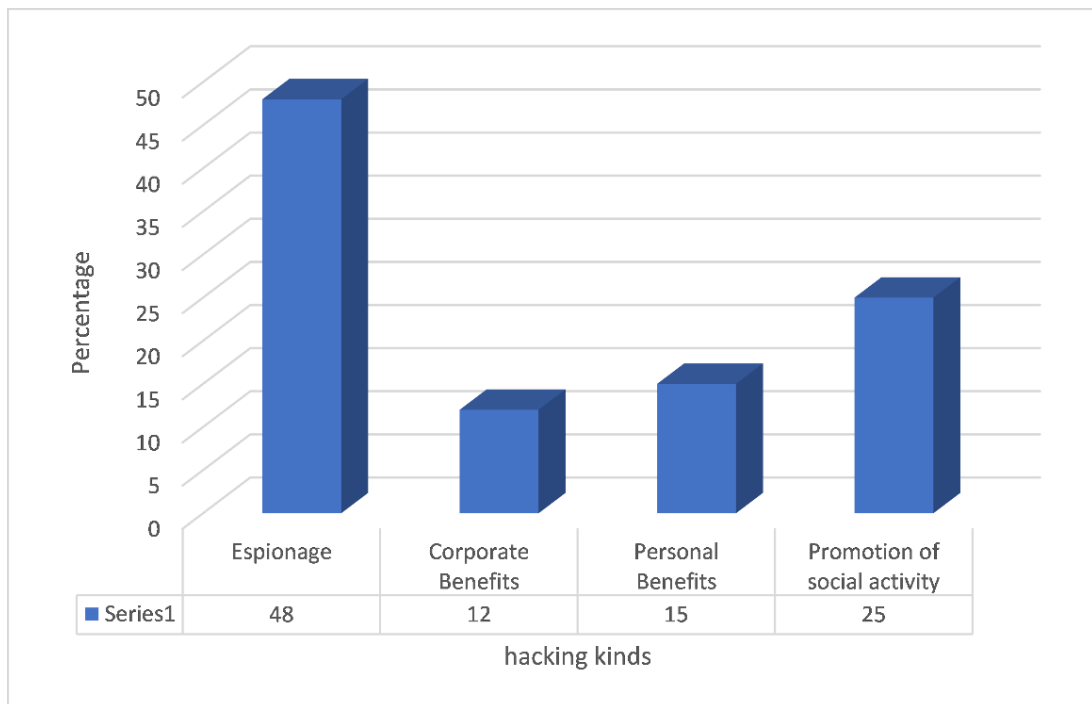
**Figure 2.2: Illustrates the global social network statistics.**

The private individuals' credentials can be sufficient for attackers in certain networks to obtain the personal addresses of the users. To maintain the breadth of the research manageable, researchers had considered prominence, therefore, reducing this same range of connections. These selected online platforms thus use cutting-edge

defensive tactics. Therefore, most potential assaults on such platforms might use cutting-edge methods [63]–[65].

### 2.3. Most penalizing kinds of data breaches

Statistics within Figure 2.3 display the attack types that are more strictly prohibited. According to that, multiple respondents responded to a study conducted throughout the US (United States) in Jan 2021. According to the research, 48% of participants agreed that the highest harsh penalties should be applied to electronic covert actions [66]–[68].

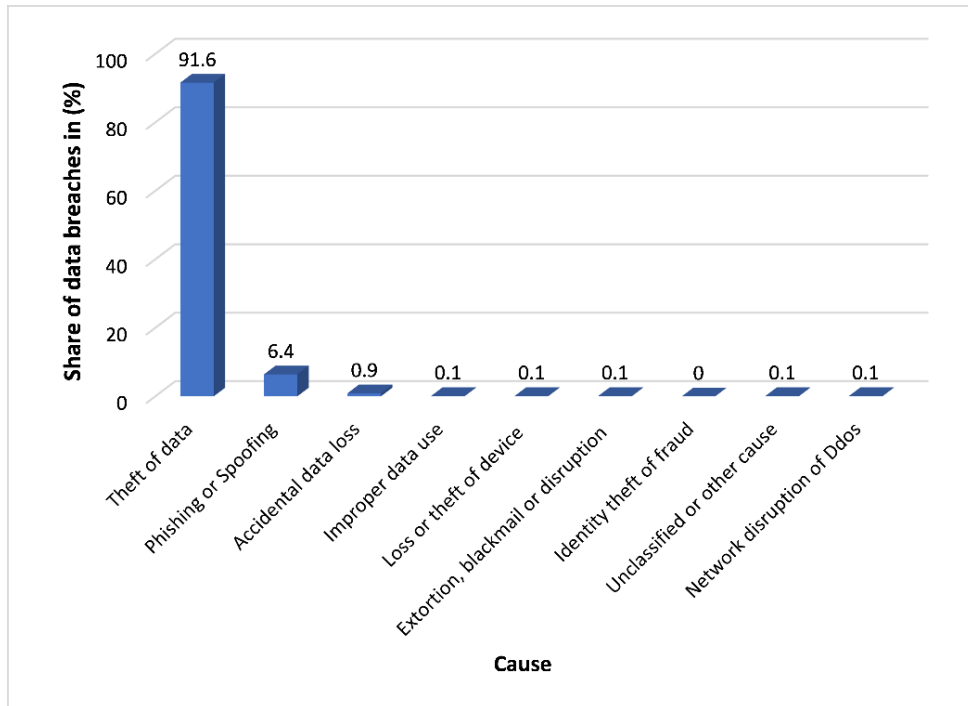


**Figure 2.3: Illustrates the most penalizing kinds of data breaches.**

### 2.4. Main reasons for dataset breach

The greatest susceptible method for data thefts globally throughout 2021 is shown in Figure 2.4. It clearly shows the share of data breach percentage. A comprehensive survey claims that 91.60% of dataset thefts ended in fraud or even the theft of credentials. Geolocation images are fairly common these times. Individuals upload images to social media sites and label those identifying actual places. Again, until users actively switch it off, many programs' geo-tagging function instantly marks the present position within a photo. By doing this, individuals attract hackers who may approach them for theft as well as expose sensitive details about themselves, such as where they reside and where they are traveling. Regularly updating personal positions

on social media might put somebody at risk for theft as well as extortion, among other dangers [69]–[71].



**Figure 2.4: Illustrates the main reasons for datasets breach [72].**

### 2.5. Credential shared by several users

The attackers abuse such confidence while multiple users communicate in real-time. Social networks may be used by attackers to influence politics and many more. The most common online networking assaults involve likejacking, wherein perpetrators add phony Instagram such as icons to websites, fraudulent websites, including junk messages.

**Table 2.1: Illustrates the datasets of individuals.**

| S. No. | Individuals Age | Individual shared credentials | Individuals not shared credentials |
|--------|-----------------|-------------------------------|------------------------------------|
| 1      | 15-20           | 44                            | 56                                 |
| 2      | 21-29           | 54                            | 46                                 |
| 3      | 30-45           | 47                            | 53                                 |
| 4      | 45+             | 24                            | 76                                 |

Table 2.1 shows the proportion of web subscribers across the US (United States). It gives insights about the nearest and dearest confidential credentials for web platforms. It is categorized through the distinct school ranges. According to the complete study, 76% of individuals who are 45 years old or older don't disclose their web credentials to relatives [73]–[75].

## **2.6. Some positive impacts of social networks on users**

Social networking has altered how people interact with one another as well as perceive the globe. Many people now use long-distance networking platforms like Facebook and Instagram to constantly remain in touch with relatives and colleagues because of their nearly global availability with little effort. Preserving societal connections, selling products and services, aiding in rescue efforts, and even locating a shared community of individuals with whom to interact and exchange ideas are just a few of the general beneficial considerations that influence one individual to develop but also utilize settings [76], [77]. Figure 2.5 illustrates the major positive impacts of social media networking. The major elements of online social media networking are described as follows.

### **2.6.1. Social Relation**

Social media online networking is constantly playing a substantial role in establishing as well as maintaining social relations in the modern era. Owing to modern technological advancements social media is rapidly connecting the world and assisting users with diverse day-to-day activities.

### **2.6.2. Grouping**

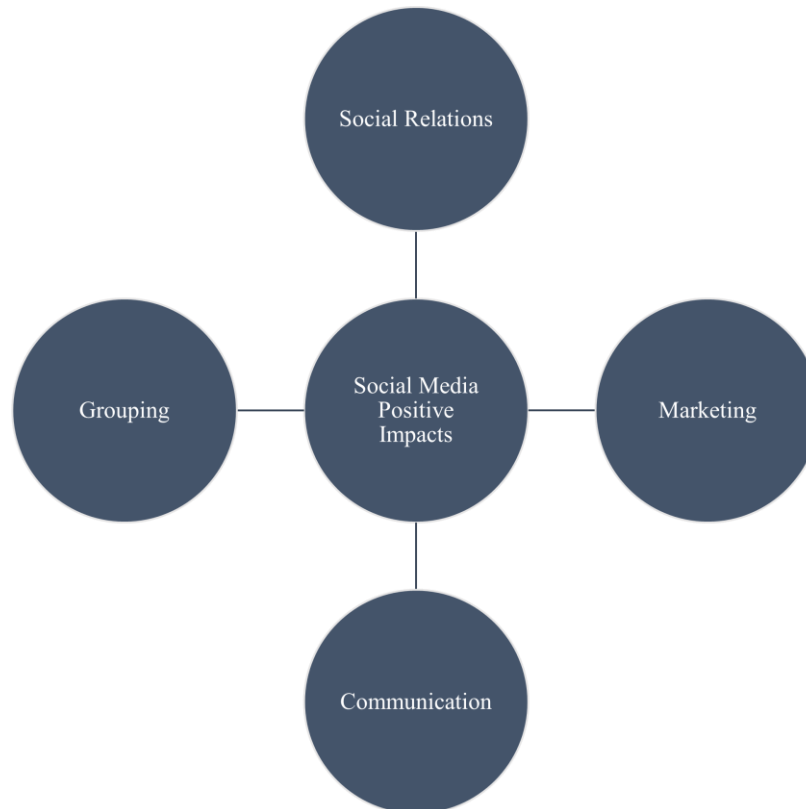
Social media networking is capable of providing a means for individuals from diverse groups to share information for work or study rapidly. This provides an effective means for the user to build multiple groups for different tasks and purposes.

### **2.6.3. Communication**

Another significant advantage of online social networking is to communicate with multiple users several times. Furthermore, people have diverse communication options namely text messaging, video calling, and audio calling options across the globe in a faster and more convenient manner.

#### 2.6.4. Marketing

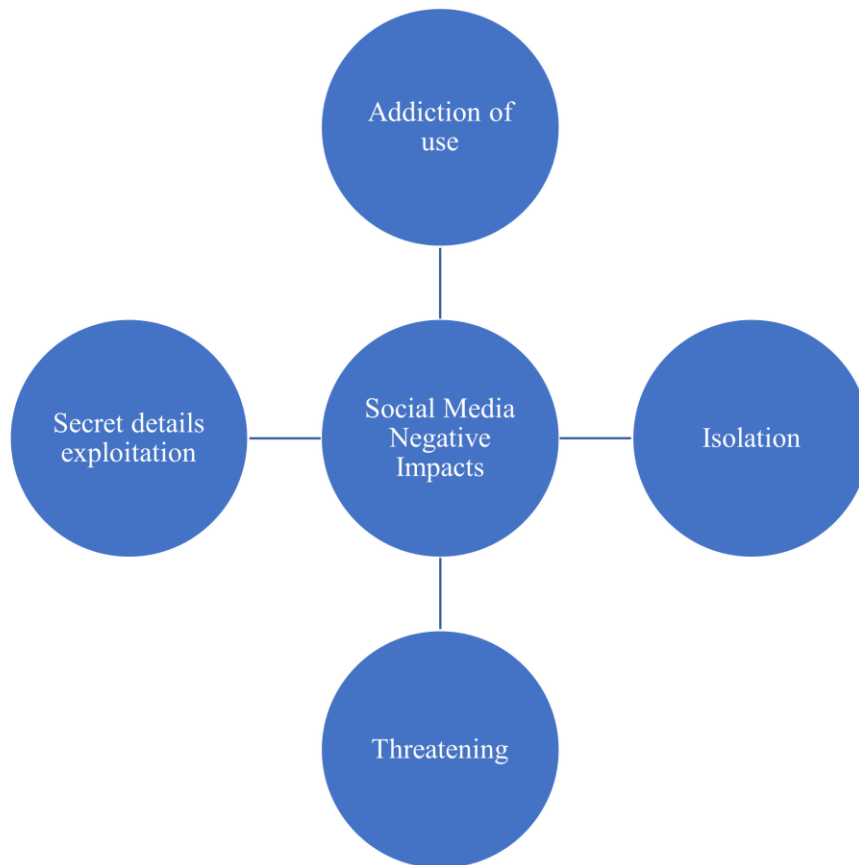
Another big advantage of online social networks is online marketing. Individuals can do their products or services marketing in a very fast manner all around the world. This also aids in the promotion of the product and services in a particular region, state, or worldwide geographical region by just clicking on a single button.



**Figure 2.5: Illustrates the major positive impacts of social media networking.**

#### 2.7. Some negative impacts of social networks on users

Social media sites with numerous new technology breakthroughs have positive as well as negative aspects. Depending upon the experts' opinions, there have been briefly discussed a few of the negative effects of online social media global networking. The overall public encounters several issues while using social media networking platforms, problems which have been identified through numerous studies depending on safety parameters. Likewise, isolation, threats, secret details exploitation, and addiction use are described as follows [78], [79]. Figure 2.6 illustrates the major negative impacts of social media networking.



**Figure 2.6: Illustrates the major negative impacts of social media networking.**

### **2.7.1. Addiction of use**

According to the research, online networking is a much stronger addiction than smoking and drinking. If individuals go an entire workday without checking their social networking sites, individuals frequently experience emptiness as well as melancholy.

### **2.7.2. Threatening**

While finding buddies online is simpler than ever, offenders may also find people quickly across social networking sites. People on social networking have consistently complained about the confidentiality offered through these platforms. Numerous individuals were only harassed in person in the past. However, bullying somebody digitally has made it possible for anybody to perform in secret.

### **2.7.3. Secret details exploitation**

Even though making a profile with social media platforms seems inexpensive, organizations primarily rely on the adverts that they display on respective web pages. Even without customers' permission, the collected information is resold to connection



agents. Additionally, attackers might use a variety of assault methods to gather confidential data regarding potential victims through such web pages.

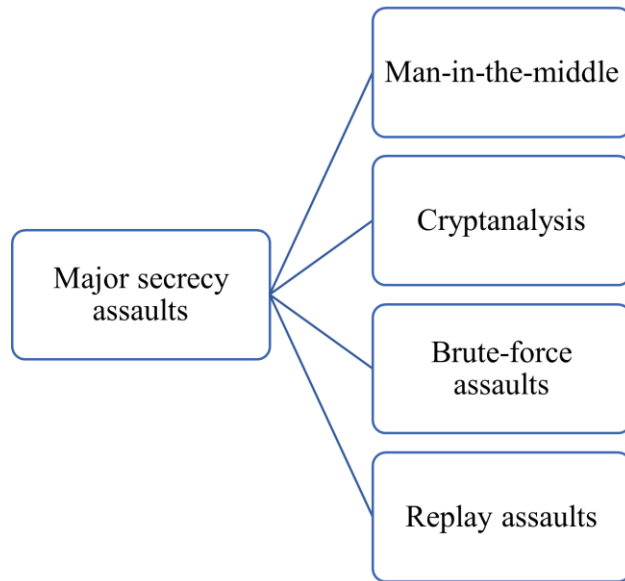
#### **2.7.4. Isolation**

Nowadays online social networking sites have undoubtedly boosted individual connections, yet it has certainly reduced in-person social engagement. Individuals find it simpler to observe the remarks made by individuals they recognize online instead of calling or visiting individuals in reality [80].

#### **2.8. Key cybersecurity assaults in social networks**

Online social networking platforms have diverse key cybersecurity secrecy assaults which are constantly becoming a major threat all around the world. Accurate secrecy and confidentiality of the user are very essential in the modern world as people share diverse essential information such as private messages, video as well as audio calls, and photos shared in groups and individual chats, etc. It is possible to trace the beginnings of communication networking and the Web to the mid-1950s and mid-1990s, respectively. Throughout the early 20th millennium, radio networks were used to join smartphone handsets to that same World Wide Web. Today, WiFi (Wireless-Fidelity) connectivity, multiple webpages, and device applications seem to be accessible on even a wide range of devices, such as smartphones and tablets, GPS (Global Positioning System) devices, etc.

This issue with dataset security within social media networking architecture, which includes verification and authorization, has indeed been identified as termed accessing management. Authorization has already been highlighted as a primary confidentiality issue within social networking sites, making cyber-secrecy concerns one of the greatest important challenges that computer platforms and social networking sites confront. This verification procedure is acknowledged as a crucial component that protects a device, network, or program against unauthorized access both immediately and implicitly. Owing to many attacks across networking throughout data transmission, especially in the global setting of social networking sites, safety, as well as anonymity, are currently constituting a major concern [81], [82]. Figure 2.7 illustrates the major key cybersecurity assaults in social networks. These kinds of major cybersecurity-related assaults on online social networking platforms include man-in-the-middle, cryptanalysis, brute-force as well as replay attacks.



**Figure 2.7: Illustrates the major key cybersecurity assaults in social networks.**

# **CHAPTER 3 SECURED THREE-PARTY AUTHENTICATION KEY EXCHANGE PROTOCOL**

## **3.1. Overview**

Advanced cryptographic protocols have been developed in response to the need for strong privacy in communication networks. The secured 3PAKE is a vital component of such protocols. The goal of this method is to safely generate a common cryptographic password amongst three participants, guaranteeing the authenticity, integrity, as well as secrecy of any information that is transferred. In contrast to the limits of conventional two-party protocols, that arise whenever used in multi-party situations, the three-party version requires new cryptography approaches to control the intricacy and guarantee increased safety. The secured 3PAKE protocol integrates a hash function and symmetric encryption to enable encrypted transmission. It is essentially a complicated arrangement of cryptography primitives. By following a well-designed set of procedures, both parties work together in unison to verify one another and jointly get an encryption key. This vital component is the pivot point for any further encrypted interaction sessions, guaranteeing that only those with the proper authorization may decode messages that are sent.

The protocol's ability to withstand several assault routes, such as replay, man-in-the-middle, as well as impersonation, highlights how effective it is in protecting channels for communication from hostile assaults. Furthermore, its flexibility to adjust to various network architectures and operating conditions makes it a flexible option for safeguarding a broad range of software, from encrypted chat systems to online transactions. The protected 3PAKE protocol has become a beacon of promise in an otherwise unsafe digital world, enabling parties to connect with assurance as risks get more complex and the technological ecosystem changes.

## **3.2. Exploration of Social Network Dynamics**

Studying social network patterns is a complex project that attempts to understand the fundamental ideas that guide activities in virtual social networks. The

examination of intricate networks made up of people, businesses, as well as other units interlinked using a variety of Internet channels, falls under this topic. Investigators aim to investigate the dynamics behind the spread of impact, group building, and knowledge in digital environments by examining both the framework and behavior of such systems.

Networking hypothesis, theory of graphs, including computer modeling are among the sophisticated quantitative techniques that are essential to the investigation of social network phenomena. With the use of such instruments, investigators may analyze complex social structures to find trends, abnormalities, and connections. Furthermore, this discipline's multidisciplinary character encourages cooperation between computer science, and sociology, among other fields, which enhances our knowledge of individual behavior in the age of technology. Utilizing methodical examination and factual research, the study of social networking interactions contributes to the advancement of theoretical understanding and provides practical approaches aimed at improving online interaction, building electronic adaptability, and encouraging ethical participation in social media networks.

### **3.3. Analysis of Existing Authentication Techniques in Social Networks**

The examination of current social network authentication methods is a critical investigation into the safety and effectiveness of the systems used to confirm individuals' identities on social media platforms online. This comprehensive analysis covers a variety of verification techniques, each having advantages and disadvantages, such as password-rooted, biometric, as well as multi-factor authentication. Utilizing methodical assessment and a comparative study, scholars seek to pinpoint deficiencies in existing methodologies and provide inventive resolutions to augment the authenticity as well as dependability of individual identification procedures.

The major goal of this study is to conduct a comprehensive analysis of how resistant authentication systems respond to various online hazards, such as phishing transactions and account takeover operations using forged passwords. Researchers can find weak places as well as devise strategies to fortify safety standards by analyzing the basic ideas and practices that underlie social network permission. Furthermore, since this is an interdisciplinary problem, experts in encoding, data security, and privacy, including human-computer interaction may work together to develop thorough methods that combine robust protection with usability. The analysis of

contemporary social networking identification techniques improves knowledge as well as safeguard's digital identity in an ecosystem wherein links are growing increasingly frequent through meticulous inspection and numerical validation.

### **3.4. Design Rationale for Dynamic Authentication Protocol**

The concept behind designing an adaptive identification mechanism embodies a nuanced strategy for dealing with the always-changing terrain of security hazards as well as user conduct. In contrast to stable verification techniques, which depend on predetermined qualifications, dynamic systems utilize behavioral patterns as well as contextual data to constantly adjust and validate individual credentials. This architectural approach stems from the understanding that advanced attacks like phishing scams, and brute force, including manipulating credentials are becoming more commonplace against standard verification techniques. Using dynamic components including gadget data, and biometric information, along with user behavior analysis, dynamic verification techniques provide a comprehensive barrier towards identity theft as well as unauthorized accessibility.

The idea of ongoing authorization, which guarantees clients are continuously authorized during their engagement with electronic devices, is fundamental to the conceptual logic of dynamic verification mechanisms. By constantly tracking client behavior and flexibly modifying verification criteria according to perceived threat stages, this strategy reduces the danger of unauthorized entry. Moreover, dynamic protocols reduce the difficulty as well as discomfort of identification procedures to maximize the overall user experience. Such standards provide a strong defense against dynamic online dangers and promote a smooth and frictionless experience for users by balancing safety and accessibility. The design logic behind dynamic verification systems, which prioritizes adaptive risk minimization and focuses on the user's design principles, essentially constitutes an entire revolution in cryptography.

### **3.5. Implementation Details and Integration Challenges**

The integration of various technological elements, operational structures, and interfaces for users can present a range of complications that pose issues in the setting of dynamic verification methods. The smooth integration of biometric devices, and multiple authentication methods, including encryption protocols into already-existing identification architectures is at the cutting edge of such difficulties. Thorough organizing, comprehensive evaluation, and attention to industry best practices are

necessary to achieve compatibility amongst different systems while upholding safety requirements. In addition, incorporation issues involve factors such as organizational behavior, acceptance among users, and compliance with regulations in addition to technical restrictions. A multifaceted strategy that involves customers from within the company and promotes innovation and teamwork is required to balance these different criteria.

Moreover, difficulties with integration can arise at any point during the authorization process, from registration and provision to authorization and revocation. There are substantial technical challenges in ensuring that consumers seamlessly switch between various identification techniques and gadgets while maintaining confidentiality and customer satisfaction. Furthermore, when businesses add more users or implement novel technologies, scaling issues become critical, requiring strong infrastructures that can handle rising needs without sacrificing safety or speed. It takes a comprehensive methodology for tackling these integration difficulties, taking into account organizational culture, stakeholder participation, technological complexity, and long-term viability. Organizations can expedite the installation and functioning of dynamic identification systems, improving security posture along with customer happiness, by proactively identifying and reducing compatibility issues.

### **3.6. User Experience and Usability Evaluation**

When it pertains to dynamic authentication methods, customer experience, and accessibility assessment provide a thorough analysis of how customers engage with systems for authentication and how well such interaction contributes to desired safety results. A variety of both quantitative and qualitative methods are used in this assessment. Investigators can acquire useful knowledge about the cognitive mechanisms and behavioral trends that influence how users interact with authenticating systems by methodically evaluating characteristics like learnability, effectiveness, and simplicity of usage. In addition, usefulness assessment goes beyond performance to include things like availability, diversity, and user autonomy, which makes systems for authentication suitable for a range of customer demographics and use cases.

The human-focused design philosophy, that puts customer requirements, choices, and abilities first throughout the planning and execution procedure, is essential to evaluating customer satisfaction and accessibility. Continually improving

login interfaces to maximize efficiency and boost user happiness is possible for programmers if they ask relevant user populations for input and apply user-centric design concepts. Furthermore, usability assessment is a crucial feedback loop that helps pinpoint problems, usability hurdles, and places where authentication mechanisms need to be improved. Organizations may promote user participation, reliability, and security by continuously improving the user interface based on factual data and user input. This will eventually boost the efficacy and uptake of dynamic identification systems.

### **3.7. Performance Metrics and Scalability Assessment**

Assessing the capacity and performance parameters of dynamic identification systems is essential to determine their viability and efficacy in real-world implementation circumstances. A wide range of quantifiable measurements are included in performance indicators, such as throughput, error rates, verification latency, as well as asset usage. Such metrics give information about how responsive and effective authenticating systems are used to determine different client demographics and workload scenarios. Furthermore, scalability evaluation looks at how well identification systems can grow with the number of users, activity volume, and system requirements without sacrificing safety or efficiency. Investigators can identify performance restrictions, structural restrictions, and inefficiencies that could prevent the widespread use and adaptability of dynamic authenticating systems by methodically assessing scalability.

The application of test-based approaches, including load measurement, stress testing, and adaptability testing is essential to evaluate the performance indicators and adaptability. To assess the durability, toughness, and adaptability of authenticating systems, such methods entail putting them under simulated workloads including stressful circumstances. Furthermore, it is possible to identify scalability boundaries and extrapolation system behavior under various circumstances by using quantitative modeling and simulation approaches. To make sure that dynamic authenticating algorithms satisfy the speed demands of real-world installation situations, investigators may arrive at well-informed judgments concerning system layout, optimization tactics, and asset distribution by measuring performance measurements as well as scaling factors. Furthermore, scalability evaluation and performance indicators are important standards to assess the dependability, effectiveness, and

scalability of dynamic identification protocols, which helps businesses implement reliable and scalable authentication systems.

### **3.8. Security Considerations in Social Network Authentication**

The intricate relationship between hostile threats, technology limits, and user behavior makes security issues in social network authentication a challenging task. Protecting customer identities, private facts, and means of communication regarding malicious activity, unauthorized availability, and information thefts is at the top of the list of priorities. Strong identification methods, insufficient encryption procedures, and vulnerability to attempts at social engineering are certain limits that must be addressed to achieve strong safety in social network settings. Furthermore, social networks' dynamic character which is marked by a quick increase in users, changing usage habits, and emerging behaviors presents special safety difficulties that call for ongoing observation, adjustment, and preventive techniques.

Deployment of multifactor verification systems, encrypting procedures, and access control rules to strengthen defenses against unauthorized access and information thefts are key safety concerns in social network verification. By reducing the possibility of identity loss and unauthorized accessibility, multifactor authorization integrates various factors including login credentials, fingerprints, and token-based authorization, thereby, strengthening the robustness of identification processes. Furthermore, end-to-end cryptography along with SSL/TLS encrypted algorithms offers a protected transmission route that protects client anonymity. By limiting employee rights and limiting accessibility to private information, access management policies such as role-rooted access control (RRAC) and the minimal privileged principle help to lessen the effect of internal vulnerabilities and unauthorized access efforts. Social network identification solutions may reduce hazards to safeguard personal information, and encourage user security and confidence in online connections by taking a holistic perspective on privacy issues.

### **3.9. Application of Dynamic Authentication in Social Networks**

Consumers' interactions and security of their electronic credentials inside web pages have undergone a fundamental change with the introduction of dynamic identification in social media platforms. Active identification techniques make use of biometrics, as well as contextual data to continually validate user credentials and identify abnormalities in real time. In comparison to conventional dynamic



authorization techniques, such systems provide improved protection and customer satisfaction by continuously adjusting authentication constraints according to customer behavior, gadget features, and ecological situations. Furthermore, dynamic verification methods offer a strong defense against fraud, hijacking of account assaults, and unauthorized access whilst facilitating easy accessibility to social media sites.

Integrating adaptive identification techniques into pre-existing verification systems is essential to the use of evolving identification in social networks. Such systems evaluate the reliability of customer visits and constantly modify identification criteria according to risk-based verification, anomaly identification, and customer profile approaches. Furthermore, dynamic identification strikes an equilibrium between safety and convenience by enabling customized security settings based on each user's unique risk assessment and usage habits. Moreover, the implementation of dynamic authenticating in social media platforms encourages a continual protection development mindset as these technologies are always learning and adjusting to new hazards and consumer behaviors. Social media platforms may improve secure stances, safeguard the privacy of users, and promote credibility and reliability in online social exchanges by using the potential of adaptive verification.

### **3.10. Advancements in Social Network Security with Dynamic Authentication**

The safety of electronic identities including confidential data inside web-based networks has entered a new age due to developments in public network encryption with variable verification. Adaptive verification is a big step forward in reducing growing cyber dangers including protecting against unauthorized access because of its flexibility and response to customer behavior and environmental clues. Dynamic verification systems provide a multi-layered defense against hijacking of accounts attempts, theft of information, as well as phishing emails by continuously altering verification constraints according to risk indicators including user location, gadget attributes, and behavioral habits.

The combination of state-of-the-art technology, strict cryptography procedures, and user-centric architectural notions is at the core of advances in social network protection with adaptive verification. Due to such developments, social media companies can implement advanced identification systems that carefully balance

protection and accessibility. Variable identification methods strengthen security against criminal activity whilst offering a smooth and flawless experience for users through the use of biometric identification, token-rooted verification, and risk-rooted access management. Furthermore, developments in dynamic verification open the door to proactively danger identification and reaction, which helps companies recognize and quickly address safety problems. Developments in dynamic identification hold great potential for guaranteeing the accessibility, anonymity, and security of client information in the age of the internet and social media platforms develop and grow.

## CHAPTER 4 LITERATURE REVIEW

This chapter provides a thorough review of multifarious existing approaches and techniques developed for maintaining the confidentiality of social networking platforms in a significant manner. Moreover, this chapter explains in detail the research gap and major limitations of the previous work done on social network secrecy. The 3PAKE techniques have previously been the subject of in-depth study throughout the past to offer privacy as well as anonymity across a variety of threats. The subsequent discourse gives an outline of the limitations of contemporary techniques.

One successful 3PAKE technique based upon an LHL-3PAKE approach was presented by the researchers, T. Y. Chang et al. [83]. Both symmetrical cryptosystems and private keys are not required through this method. This approach has many drawbacks, including the absence of bilateral verification between clients, and authorized providers don't ever reveal a backup account password in the event of a lost meeting code.

O. Ruan et al. [84] formalized confidentiality proof inside the standard paradigm while describing an alternative LR eCK confidentiality argument for 3PAKE and suggesting a better LR 3PAKE method. This method is appropriate yet simple to employ across a wide range of networking systems, but it contains several limitations, including significant computational overhead and a limited ability to provide confidentiality outside of the prototype settings without overflow attacks.

In [85], C. T. Li examined Farash-system Attari's scheme and demonstrated how private information is retained on an authorized application server. This approach cannot offer protection over security method leak attacks. The researchers of the current study reduced the dangers to Farash-system Attari's that still existed, although the offered solution still offers concealment in transmission cost and computational difficulty environments.

Some shortcomings of earlier work by Lee et al. on confidentiality systems were previously revealed by M. S. Farash et al. [86], who also examined the necessity for

new and secured 3PAKE algorithms designed for augmentation in a better practical way. The researchers placed forth a moderate response which keeps the computing power and connectivity effectiveness of the previously recommended method. Nevertheless, this explored methodology provides less confidentiality over various attacks, such as man-in-the-middle and cryptanalysis assaults in the context of social networking infrastructure.

In [87], Q. H. Zhang and colleagues explored and assessed the verified-based 3PAKE technique, which maintains the secured password validator in addition to the simple secured script upon this authorized site. Nevertheless, in the context of underlying social network infrastructure, this technique fails to provide the necessary confidentiality towards directory attacks, man-in-the-middle attacks, etc.

In [88], the authors Q. Xie and colleagues proposed an improved 3PAKE technique which is based on a chaotic map model. While this enhanced approach has certain improvements above current privacy techniques which rely on verified client private confidentiality credentials. However, this approach is less effective due to the higher computational intricacy of social networks.

Another light-weight and reduced computing cost 3PAKE technique based on a single XOR (Exclusive OR) function was explored by C. Y. Lin et al. [89]. This technique offers confidentiality over spoofing attacks, cryptanalysis assaults, etc. This technique is harmed by common credential theft via authorized hosts as a result of the very rapid advancement of various applications, including cloud-based and ubiquitous computer technology, devices with lesser processing capacity, etc.

A further efficient 3PAKE approach based on the intelligent cards, and cryptographic HF, was proposed by R. Amin et al. [90]. The researchers reviewed the collection of research to pinpoint the major issues of data leakage while transmission as a result of different attacks. Even though this primary use for the research method involves bilateral identification between both users and servers, it nonetheless does have a significant computational overhead when used in actual operations across a wide range of fields.

Furthermore, an improved 3PAKE with enormous transmission effectiveness and increased secret grade in several settings and implementations was presented by Q.

Shu et al. [91]. However, this approach has some restrictions relating to online social networking platforms' privacy.

Another upgraded 3PAKE approach based upon that chaotic-based map for the upgraded confidentiality threshold was proposed by C. M. Chen et al. [92]. However, the recommended technique is susceptible inside the social media networking setting due to a variety of attacks including man-in-the-middle attacks, relay attacks, etc.

Time Password (OTP) rooted client verification strategy was implemented by S. Lone and colleagues [93]. For achieving overall needed concealment, the recommended strategy has been put into practice and verified by utilizing Android-based smartphone devices. This recommended technique, nevertheless, has specific limitations, including the possibility of customer information leaking if an OTP gets misused and a lack of reliability when exchanging private information through digital media.

Furthermore, extensive research on the 3PAKE technique to guarantee required secrecy and confidentiality throughout a range of cyber-assaults has been done. This 3PAKE exploration provides a list of acknowledged approach shortcomings. In [84], O. Ruan and colleagues successfully showed a 3PAKE approach that is based on the SE approach. Similar to symmetric cryptography systems, the proposed 3PAKE technique doesn't call for a common passcode. This method has several drawbacks, along with the difficulty of disclosing a backup passcode in case identification credential gets stolen and lacks customer and operator authentication.

Furthermore, another 3PAKE protocol is modified by R. Muthumeenakshi and colleagues [94] for data security in the vehicular ad hoc network (VANET) setting. This VANET seems to be merely a cellular connection made up of faster cars that can create a connection to one another via an integrated broadband connection. Both conventional transmission means and information validation failing circumstances allow the enhanced method to deliver the requisite confidentiality. This technique's primary flaw is that this cannot offer optimal data security against cryptanalysis assaults during transmission.

Further, a 3PAKE method is disclosed by Q. Shu and colleagues [91]. This proposed 3PAKE approach is based on the ideal lattice. To share protected data through real-time conversation through social networking sites, many users must set secured

login credentials utilizing authorized distant servers. This is necessary owing to the fast expansion of virtual media platforms in the modern world. The client's interaction confirmation passcode has been necessary for earlier investigated methods, and it is usually kept within the host databases. However, the stored credentials on the computer servers can be accessed by various information leakage strategies applied by hackers. Consequently, inside the current public networking context, the existing approach is incapable of offering the necessary confidentiality.

A novel 3PAKE technique was described by J. Zhao and colleagues [95], for enabling safe information sharing in real-time. Nevertheless, this methodology is unable to achieve the necessary confidentiality since it uses a traditional hash-function algorithm. The main issue with this social network approach is the confidentiality of customer identification. The attacker might be able to identify the customer's credentials in real time. The hash-function-based 3PAKE algorithm has some security limits in social networks due to high data breach attacks over the network such as cryptanalysis attacks etc.

In research [96], M. Kim and colleagues investigated a customized 3PAKE method to provide anonymity during data transmission over social networks. These protocols have been implemented to protect medical records during actual transmission. However, it has several privacy-related issues since the solutions provided cannot handle user confidentiality in real-time.

In [97], H. Xiong and colleagues explored an updated 3PAKE technique for server-based secret information sharing. Nevertheless, the current technique is unable to handle several assaults like Keys compromise impersonation (KCI) assaults and contains several flaws connected to safe information confidentiality.

Although in certain social network settings, in which there are fewer chances for assaults while the connection with the authorized client, such types of previous techniques guarantee the secrecy of the shared information. Due to cryptographical assaults and man-in-the-middle assaults, when data gets translated through social networking sites, the previously explored 3PAKE systems contain several flaws related to high computing costs and credential breaches. In daily practice, individuals use particular social networks to transmit a wide variety of private datasets due to the huge

volume of transactions across the verified system. There is a considerable risk of dataset leaking through different offenders during the actual connection.

Therefore, the creation of a revolutionary 3PAKE technique that may eliminate any possibility of cross-connection attacks during real-time data exchange using any authorized host is necessary to address these sorts of issues. Additionally, there exists a need for advanced 3PAKE approaches that provide better reliability and safety in social network environments with a greater risk of data leaks which give greater anonymity to users whenever multiple users communicate with one another [25–27]. Table 4.1 illustrates the existing state-of-the-art techniques used for security verification and their drawbacks.

**Table 4.1: Illustrates the existing state-of-the-art techniques used for security verification and their drawbacks.**

| <b>S. No</b> | <b>Name of Author</b> | <b>Publication Year</b> | <b>Technique Used</b>  | <b>Drawbacks</b>  |
|--------------|-----------------------|-------------------------|--|---|
| <b>1</b>     | Ruan et al. [84]      | 2019                    | SE as well as HF   | This technique is incapable of revealing a substitute to access the passcode while the user communicates. |
| <b>2</b>     | Xie et al [88]        | 2015                    | Chaotic-based maps   | Unable to handle key guessing-based assaults over the authentic communication server.                     |
| <b>3</b>     | Shu et al. [91]       | 2021                    | Modified Ideal-lattices approach                             | Minimal computing and communication competence.   |
| <b>4</b>     | Li et al. [85]        | 2018                    | Enhanced-Quadratic residues and Chebyshev chaotic-rooted map | Incapable of defending against a passcode disclosure attack.  |
| <b>5</b>     | Zhao et al. [95]      | 2012                    | Improvised-Trapdoor testing approach                         | The enhanced protocol offers huge computing complexity and greater execution time.                        |
| <b>6</b>     | Kim et al. [96]       | 2020                    | New-Biometric-rooted key interchange                         | Apprehensive against insider assaults along with impersonation attacks in real-time.                      |

|           |                               |      |   |   |
|-----------|-------------------------------|------|---|---|
| <b>7</b>  | Muthumeenakshi et al. [94]    | 2017 | Server-user based-authentication procedure and batch messaging dispatches | Large transmission overload along with service interruption.                |
| <b>8</b>  | Xiong et al. [97]             | 2013 | HF as well as none server-based public passcodes                          | This method is incapable of managing multifarious assaults such as KCI etc. |
| <b>9</b>  | Ikhaliya et al. [101]         | 2019 | Chaotic-maps  | High computing complexity in network maintenance.                           |
| <b>10</b> | G. Rathee et al. [102]        | 2021 | Hypothetical mathematical archetypal                                      | More time consumption   |
| <b>11</b> | C. Borrego et al. [103]       | 2019 | Homomorphic encryption  | Less secure on large datasets   |
| <b>12</b> | S. Mostafi et al. [104]       | 2019 | Social Internet of Things (SIoT)  | Fails to manage high traffic during peak hours                              |
| <b>13</b> | G. Yan et al. [105]           | 2011 | Location-based online social network                                      | Fail to handle various real-time assaults                                   |
| <b>14</b> | Y. Chen et al. [106]          | 2018 | Malware spread model  | More time-consuming model performance assessment                            |
| <b>15</b> | E. Ikhaliya et al. [107]      | 2014 | Improved OSN model  | Low accuracy  |
| <b>16</b> | S. K. Sheoran et al. [108]    | 2021 | ML-Based optimized scheme   | Lower precision rate  |
| <b>17</b> | A. O. et al. [109]            | 2020 | Epi Model network simulation  | More computational complexity   |
| <b>18</b> | M. R. Faghani et al. [110]    | 2019 | An analytical model   | Less resistant against real-time attacks                                    |
| <b>19</b> | M. R. Faghani et al. [111]    | 2013 | Selective monitoring scheme   | Lower trusted   |
| <b>20</b> | N. Venkatachalam et al. [112] | 2017 | Steganography and host-based method                                       | More time consumption   |
| <b>21</b> | H. Zhu et al. [113]           | 2014 | New MPPM model for OSN security   | Less trusted in modern OSN infrastructure                                   |



#### 4.1. Review of Chun-Ta-Li 3PAKE protocol

This research has reviewed and analyzed the existing Chun-Ta-Li [85] research work. This study was conducted for the 3PAKE protocol with client anonymity rooted in the chaotic map approach. It is observed that the passcode alteration process is less secure in recognizing the validity invitation while the insecurity in the passcode alteration stage might root the offline passcode guessing assaults. For the elimination of such assault's drawbacks, rooted on quadratic residues and Chebyshev chaotic maps, there is a developed new 3PAKE protocol rooted on chaotic maps. The steps of the suggested 3PAKE protocol along with user anonymity are summarized as follows:

*Phase 1: Registration Process:*

Step 1: The user selects key identification  $ID_e$  and passcode denoted as  $PC_s$  as well as compute the  $PC_w = TS_{pwi}(\alpha) \bmod p$  as well as  $H(RN_{ip}, PC_w)$ , wherein the term  $RN_{ip} \in [1, pt + 1]$ . Further, the client generates a request for registration  $\{ID_e, H(RN_{ip}, PC_w)\}$  to the authenticated server  $S_{AU}$ .

Step 2: Authenticated server  $S_{AU}$  calculates the  $V_x PC_w = H(ID_e, S_{AU}) + H(RN_{ip}, PC_w) \bmod pt$  and saves  $(ID_e, V_x PC_w)$  in the database as well as  $H(RN_{ip}, PC_w)$ .

Step 3: Authenticated client saves  $RN_{ip}$  in the end-user gadget.

*Phase 2: Authentication Process:*

While client  $A_1$  and client  $A_2$  want to authenticate arbitrarily and generate the same session code, the following steps are executed.

Step 1: Client  $A_1$  selects an arbitrary number defined by  $R_A \in [1, pt + 1]$  and input the passcode  $PC_w$ . Further,  $A_1$  calculate the  $R_A = T_{rA}(\alpha) \bmod p$ , and  $PC_w = TPW_A(\alpha) \bmod pt$ .

Step 2: While  $Ma_1$  is obtained from the authenticated server  $S_A$ , it is revealed by utilizing the remainder theorem having the variables  $X_a$ , and  $Y_a$ . Further, the  $S_A$  verifies the stored values.

Step 3: While the  $Ma_2$  is obtained from  $S_A$ , Client  $A_2$  inputs the generated passcode  $PC_w$ , and evaluate the  $H(RN_{ip}, PC_w)$ , wherein the  $RN_{ip}$  is retrieved from the end user gadget.

Step 4: While the  $Ma_3$  is obtained from  $A_2$ ,  $S_A$  reveals that  $Ma_3$  utilizes the remainder theorem having  $X_a$ , and  $Y_a$ , to attain the  $(ID_{X1}, ID_{X2}, ID_{X3})$ .

Step 5: Once the  $Ma_4$  is obtained from the  $S_A$ ,  $A_1$  estimates the  $K_{ASa} = TR_{A1} \text{ mod } pt$ .

Step 6: While the  $Ma_5$  is obtained from the  $S_A$ ,  $A_2$  estimates the  $K_{ASa} = TR_{A2} \text{ mod } pt$ .

Step 6: After obtaining the  $Ma_6$  from the authenticated  $S_A$ , there is verified the computed  $(ID_{X1}, ID_{X2}, ID_{X3})$ . While it is found valid, then only the  $S_A$  is authenticated through the  $A_2$ .

*The procedure of the proposed 3PAKE protocol:*

The key steps of the proposed 3PAKE protocol have been described as follows:

Stage 1: CA selects one arbitrary numeral  $a \in Tp$ , evaluates  $d^{a_n}$  and one occurrence password  $Ha(CA, d^{a_n}, PWax)$ , obtains,  $REQA = CA, d^{a_n}, \{CA, d^{a_n}\}Ha(CA, d^{a_n}, PWax)$  at that moment translates  $REQA$  towards the authenticated CB.

Stage 2: Through receiving the records from CA, then the CB instantly validates the individuality of  $d^{a_n}$  as well as later CB chooses another randomized numeral  $bn \in Tp$  but also the numeral employed on one occasion  $Nu$ , assesses  $d^{b_n}$  then one occurrence passcode  $Ha(CB, d^{b_n}, PWbx)$ , gets,  $REQB = CB, d^{b_n}, \{CB, d^{b_n}\}Ha(CB, d^{b_n}, PWbx)$ .

Stage 3: Through receiving the  $REQB$  as well as  $REQA$ , authentic host  $Sa$  firstly confirms this individuality of  $d^{a_n}$  as well as  $d^{b_n}$ , later genuine host  $Sa$  apply received  $d^{a_n}$  and  $d^{b_n}$  for evaluation  $Ha(CA, d^{a_n}, PWax)$  as well as  $Ha(CB, d^{b_n}, PWbx)$  command through and later in subsequent phases decodes this  $REQA$  as well as  $REQB$  for verifying and validating  $d^{a_n}$  along with the  $d^{b_n}$ .

Stage 4: The CA decodes  $CAKa$ , then gets the  $d^{a_n v_n}$  as well as  $Nu$  assesses, and the  $CK = (d^{b_n v_n})^{a_n} = d^{a_n b_n v_n}$ , later receives  $\{CA, Nu, d^{a_n}\}C_K$ , and translate the  $CAKb$ ,  $\{CA, Nu, d^{a_n}\}C_K$  towards the user CB.

Stage 5: Through receiving the  $CAKb$ ,  $\{CA, Nu, d^{a_n}\}K$ , originally then the user CB decodes the code  $CAKb$  for obtaining the  $d^{a_n v_n}$  as well as, later validate  $d^{b_n}$ .

Stage 6: At last, both the chosen client CA along the client CB identify another new session passcode i.e.,  $C_K$  to furthermore chat and then get rid of the probabilities of real-time records of fatalities within the social networking models.

This is evident from the comparative analysis of the proposed 3PAKE protocol with the existing Chun-Ta-Li 3PAKE protocol that multifarious merits emerge. Initially, the enhanced 3PAKE protocol provide a well-established architecture with improved security. Further, robust data secrecy is offered, while the hash function gives integrity validation over the server. Additionally, the enhanced 3PAKE protocol provides faster computing time and minimal computational overhead in comparison to the chaotic map-based anonymous user verification protocol developed by Chun-Ta-Li, thereby improving the overall performance of the developed protocol in resource-constrained settings.

#### **4.2. Problem Identification**

People are always looking forward to more affluent lifestyles because intelligent data systems become more prevalent. Prominent intelligent data frameworks encompass mobile telecommunications, the Web, wearable technology, etc. In several such scenarios, there are several advanced terminals, including smartphones and other computing devices. While user A, and user B, want to establish a secure link, each must first work with the host to generate powerful bilateral encrypted credentials for the link. This 3PAKE technique is known as a method of safe information exchange among various participants. The 3PAKE approaches offer several benefits together in a variety of settings worldwide. Furthermore, 3PAKE techniques allow safe information exchange and collaborative validation. For instance, a certified trustworthy web server supports communications between providers and customers during e-commerce transactions, etc. Numerous types of confidentiality techniques have been investigated to provide secret information communication and necessary privacy. Nevertheless, the majority of methodologies have a variety of restrictions as a result of the quick alterations in connectivity architecture in real-time. As a result, the current procedures are unable to handle major threats namely man-in-the-middle assaults, cryptanalysis, and others inside the data transmission process, which calls for significant recognition of this problem.

The advanced 3PAKE protocols to address all such previously recognized problems have been implemented in this work. These protocols give users advanced security while exchanging vital data over social networking sites. The enhanced 3PAKE protocol is responsible for managing previously noted attacks throughout conversation in an extremely short amount of period. Social network security has

become very intricate in the modern world owing to server security attacks. In this research, an enhanced 3PAKE protocol is implemented for online social network security verification. This proposed enhanced 3PAKE protocol is based on the SE and HF which is capable of managing various attacks on social networks. This enhanced 3PAKE protocol is built to integrate with the real-time social network communication model. Moreover, the 3PAKE protocol performance metrics have been obtained highly optimal and compared with the state-of-the-art 3PAKE methods. It is observed from the accessed techniques that the proposed technique is more robust against distinct security attacks and provides less computational complexity.

### **4.3. Objectives**

The privacy of social network models is a critical threat in the modern era. As internet users are increasing worldwide continually, therefore the secrecy concerns of social networks at present have become serious issues in maintaining the confidentiality of the user profile and essential information exchange in communication. In considering these major problems of social networks, there is a need to build a significant and higher level of protocols for the social network models that are more reliable in terms of privacy and confidentiality of the important credentials of the users. Moreover, there is a need to authenticate the users in real-time communication for authorization purposes to maintain the entire network secrecy and eliminate the chances of the network secrecy breach by developing novel advanced-level 3PAKE protocols having very minimal computing complexities and less processing time.

- To study various security as well as trust computation techniques for social network models.
- To design and develop a security framework for a secure network.
- To compare and validate the proposed security framework with the existing framework.

### **4.4. Research Contributions**

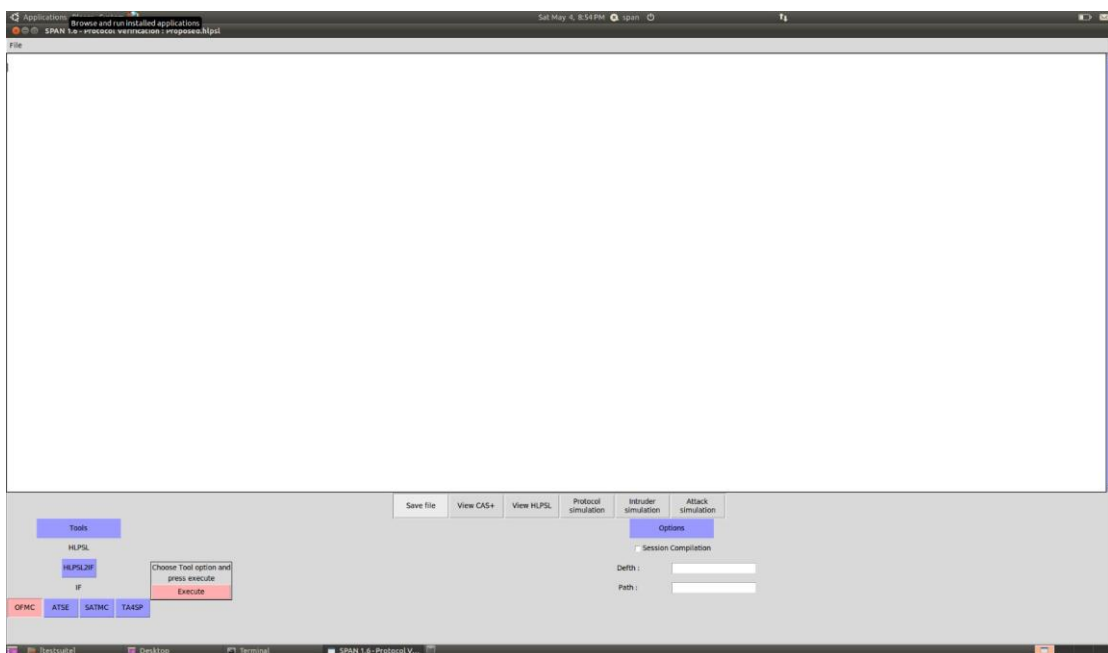
This thesis provides a pragmatic solution for greater secrecy and confidentiality of the users while exchanging information such as text messaging, audio as well and video calls including the users' profile information in social network settings. In this work, two diverse secrecy protocols have been implemented.

- The first secured and enhanced 3PAKE (Three-Party Authenticated Key Exchange) technique was developed rooted in symmetric encryption (SE) and hash function (HF). Secondly, another 3PAKE advanced-level secrecy protocol has been built on the combined approach of elliptic curve cryptography (ECC) and SE.
- The social network model provides anonymity i.e. individual's identity is concealed whenever common connections are employed in the communication process, thereby user credential secrecy and confidentiality are maintained precisely.
- Both of the implemented 3PAKE algorithms promise greater confidentiality against various assaults including brute-force assaults, man-in-the-middle, and parallel assaults. Therefore, the developed 3PAKE protocols intended to improve runtime metrics like parseTime, searchTime, depth-plies, and visited nodes by decreasing the execution cycles.
- This research aims to provide enhanced 3PAKE algorithms with reduced processing times, minimal processing overhead, and resistance to multifarious assaults, thereby, improving the transmission efficiency practically.
- The conventional techniques have multifarious restrictions related to the secrecy and privacy of the user-secured communication and credentials against distinct real-time attacks by hackers on the authenticated server. A few of the most common attacks may include man-in-the-middle, brute-force attacks, etc. This proposed 3PAKE approach is highly confidential and secured in terms of data secrecy breach and executes fast in real-time.
- To address security-related problems, multiple 3PAKE protocols have been developed and validated with greater precision. This developed approach uses the extremely minimal time to handle the large quantity of data through social networks while providing increased privacy to the user-secured credentials over the secure database of the server.

# CHAPTER 5 PROPOSED WORK (HYPOTHESIS)

## 5.1. AVISPA Software

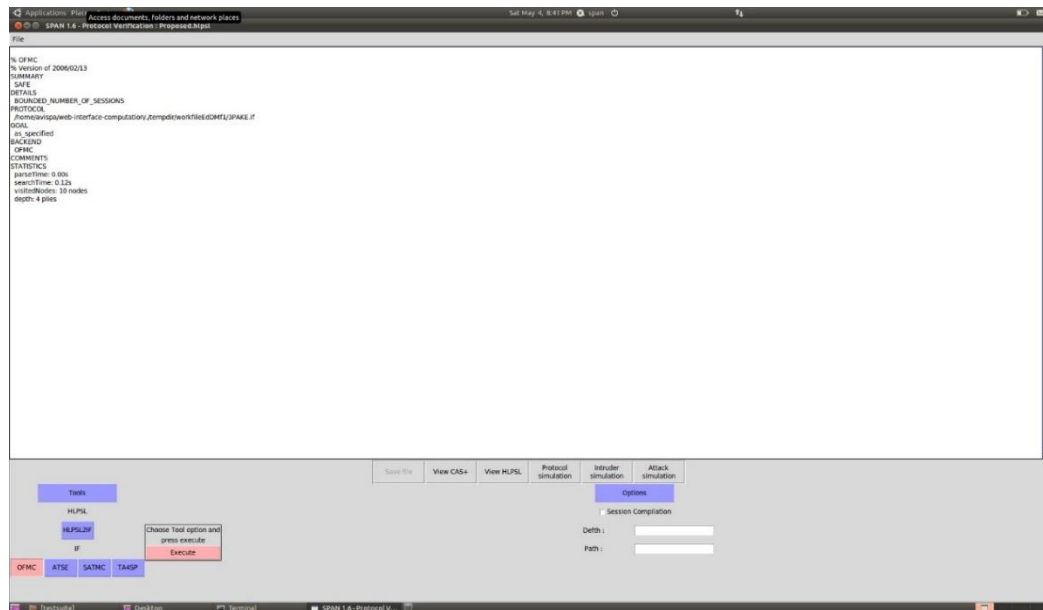
The widely-used Automated-Validation of Internet Security Protocols, and Applications (AVISPA) platform has been used to implement enhanced 3PAKE protocol for the social network model which allows to authorize anonymity and confidentiality attributes. This enhanced 3PAKE protocol has been developed to verify multifarious user credentials and secure information over social network models. This AVISPA software utilizes a push-based button to validate confidential and secrecy-sensitive 3PAKE protocol for the social network model. This enhanced 3PAKE protocol is defined inside the commonly used AVISPA tool using the Higher-Level Protocols-Specification Languages (HLPSL). Figure 5.1 depicts the interface of the AVISPA software.



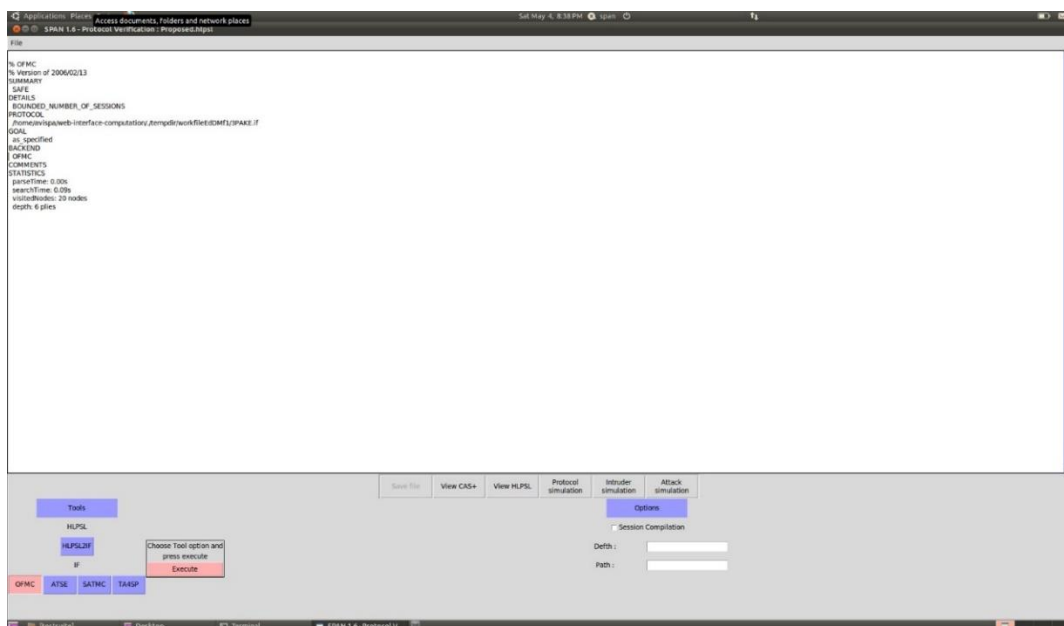
**Figure 5.1: Depicts the interface of the AVISPA software.**

Various privacy settings were set and responsibilities were assigned throughout the HLPSL program. When 3PAKE protocol implementation procedures have been executed, the basic responsibilities are typically utilized to specify the overall actions of any stand-alone entity. During the protocol implementation and validation, various

tasks outline a whole protocol loop, and protocol sessions between many actors, or the protocol modeling themselves is done precisely for optimal observation of the performance metrics. It is essential to fix the AVISPA setting scenario before the execution of the protocol. To utilize multiple functions for 3PAKE protocol verification, it is vital to determine the specific session meetings. Figure 5.2 depicts the 3PAKE protocol verification summary on 10 nodes. Figure 5.3 depicts the 3PAKE protocol verification summary on 20 nodes.



**Figure 5.2:** Depicts the 3PAKE protocol verification summary on 10 nodes.



**Figure 5.3:** Depicts the 3PAKE protocol verification summary on 20 nodes.

## 5.2. Limitations of the AVISPA tool

When utilizing the AVISPA tool to implement the 3PAKE protocol for social networks, there are a few built-in constraints that are recognized. Although AVISPA is a powerful tool for cryptographic protocol assessment, its limitations have been stated for a thorough grasp of the research process.

- One vital limit of the AVISPA tool is restricted support for customized or specialized cryptography algorithm analysis in case the developed algorithm is intricate and larger.
- The user interface of the AVISPA software is complex which poses threats for researchers in experimental analysis with limited expertise.
- New protocol constraint requires careful consideration while choosing the protocols for evaluation, as distinct niche or non-standard protocols might fall outside the purview of AVISPA software competencies.
- Moreover, AVISPA software scalability might present a bottleneck while evaluating the larger or more complicated cryptographic algorithms.
- The computing assets and time needed for evaluation might become arbitrarily large as the number of steps and complexity of the procedure expand, thus hindering the effectiveness of the investigation approach.
- Therefore, while choosing protocols for implementation, investigators need to be cautious and think about how the selected technique might impact scalability.

## 5.3. Advantages of the AVISPA tool

The crucial advantages of the AVISPA simulation tool are described as follows:

- AVISPA tool empowers researchers and developers with a heightened level of confidence in the secrecy of 3PAKE protocols by providing rigorous verification settings that thoroughly scrutinize all aspects of the protocol's design and implementation.
- With AVISPA's adaptable analysis methods, users might handle the verification procedure to focus particularly on the distinct attributes and secrecy necessity of the 3PAKE algorithm, ensuring that potential vulnerabilities have been addressed and identified properly.
- AVISPA offers comprehensive coverage of secrecy properties related to the 3PAKE protocols, which involve authentication, secrecy, and integrity,



enabling a complete evaluation and verification of protocol security across multifarious settings.

- Through the automated analysis method and offering intuitive interfaces, the AVISPA tool streamlines the development of 3PAKE protocols, thereby, allowing researchers to identify and rectify security threats early in the design stage to secure time and resources.
- AVISPA remains a reliable tool, providing the flexibility and scalability to accommodate evolving algorithm specifications and analysis necessities, thus ensuring continued assurance of algorithm secrecy over time.

#### **5.4. Protocol 1- Enhanced 3PAKE Protocol**

In this research, the first diverse security, and trust computation approaches for the social networking model have indeed been studied. Further to maintain the secrecy and the confidentiality of the social network models, initially an enhanced 3PAKE protocol was developed rooted in the SE as well as HF.

##### **5.4.1. Notions utilized**

Sa stands for a reliable host. Two different individuals named CA, as well as CB, wish to communicate safely with each other using this same Sa. This same recommended 3PAKE protocol was developed throughout this investigation using the DHKE (Diffie-Hellman Key Exchange) technique and therefore is centered on HF as well as SE. The secured method of exchanging cryptography keys over a public network is called DHKE.

This recommended approach was built using the DHKE technique, hence a specific cyclic clustering namely the  $(CG, e, f)$  which was also generated by an element  $e$  of foremost value  $f$  should be selected. Client CB randomly selects  $Nu$  as a digit to ensure the overall novelty of such a system. Inside a validation process, this same  $Nu$  is typically any pseudo-random or randomized integer assigned to ensure whether the preceding transmission cannot be used more than once against different attacks. These abbreviations utilized as well as associated meanings are shown in Table 5.1.

**Table 5.1: Illustrates the notations used and their definitions.**

| S. No. | Notation        | Definition   |
|--------|-----------------|--|
| 1      | $(C_G, e, f)$   | Definite cyclic cluster $C_G$ created via a component $e$ of prime order $f$ |
| 2      | $C_A$ and $C_B$ | Two users that also denote their own uniqueness                              |
| 3      | $PW_{ax}$       | Symmetric key exchanged between $C_A$ and S                                  |
| 4      | $PW_{bx}$       | Symmetric key exchanged between $C_B$ and S                                  |
| 5      | $N_u$           | An arbitrary number utilized once by $C_B$                                   |
| 6      | $S_a$           | Authenticated server   |
| 7      | $Ha(M)$         | Confidential unilateral hash function  |
| 8      | $\{M\}_{ka}$    | Ciphertext that symmetric encrypt $M$ along with $ka$                        |

#### 5.4.2. Design Enhanced 3PAKE Protocol

Multiple individuals  $CA$ , as well as  $CB$ , want to transmit a unique access token  $Ck$  for their succeeding transmission employing this improved technique, alongside the help of host  $Sa$ . Users  $CA$ , as well as  $CB$ , are not directly authenticated with one another. Users must turn to the authorized host  $Sa$  to negotiate again for secured access credentials.

This same flowchart of the improved 3PAKE approach for socializing networking that uses an HF as well as SE is shown in Figure 5.4. Following is a detailed explanation of each stage within our recommended 3PAKE methodology:

Stage 1:  $CA$  chooses one randomized numeral  $a_n \in T_p$ , assesses  $d^{a_n}$  and one occurrence passcode  $Ha(CA, d^{a_n}, PW_{ax})$ , receives,  $REQA = CA, d^{a_n}, \{CA, d^{a_n}\}Ha(CA, d^{a_n}, PW_{ax})$  at that moment translates  $REQA$  towards the  $CB$ .

Stage 2: Through receiving the records from  $CA$ , then the  $CB$  instantly validates the individuality of  $d^{a_n}$  and later  $CB$  chooses another randomized numeral  $b_n \in T_p$  but also the numeral employed on one occasion  $N_u$ , assesses  $d^{b_n}$  then one occurrence passcode  $Ha(CB, d^{b_n}, PW_{bx})$ , gets,  $REQB = CB, d^{b_n}, \{CB, d^{b_n}\}Ha(CB, d^{b_n}, PW_{bx})$  at that time translates the  $REQA$  and  $REQB$  toward the valid data handling server  $Sa$  in real-time.

Stage 3: Through receiving the REQB as well as REQA, authentic host Sa firstly confirms this individuality of  $d^{a_n}$  as well as  $d^{b_n}$ , later genuine host Sa apply received  $d^{a_n}$  as well as  $d^{b_n}$  for evaluation  $\text{Ha}(\text{CA}, d^{a_n}, \text{PWax})$  and  $\text{Ha}(\text{CB}, d^{b_n}, \text{PWbx})$  command through as well as later in subsequent phase decodes this REQA and REQB for verifying as well as validating  $d^{a_n}$  along with the  $d^{b_n}$ . While, unsuccessful verification, the entire session would halt immediately, else this authorized host Sa chooses any randomized numeral value  $v_n \in \text{Tp}$ , assesses  $d^{a_n v_n} = (d^{a_n})^{v_n}$ ,  $d^{b_n v_n} = (d^{b_n})^{v_n}$  as well as gets  $\text{CAKa} = \{d^{a_n}, \text{CB}, d^{b_n v_n}, \text{Nu}\} \text{Ha}(\text{CA}, d^{a_n}, \text{PWax})$ ,  $\text{CAKb} = \{d^{b_n}, \text{CA}, d^{a_n v_n}, \text{Nu}\} \text{Ha}(\text{CB}, d^{b_n}, \text{PWbx})$ , but also, at the end translates CAKa as well as CAKb towards this CA.

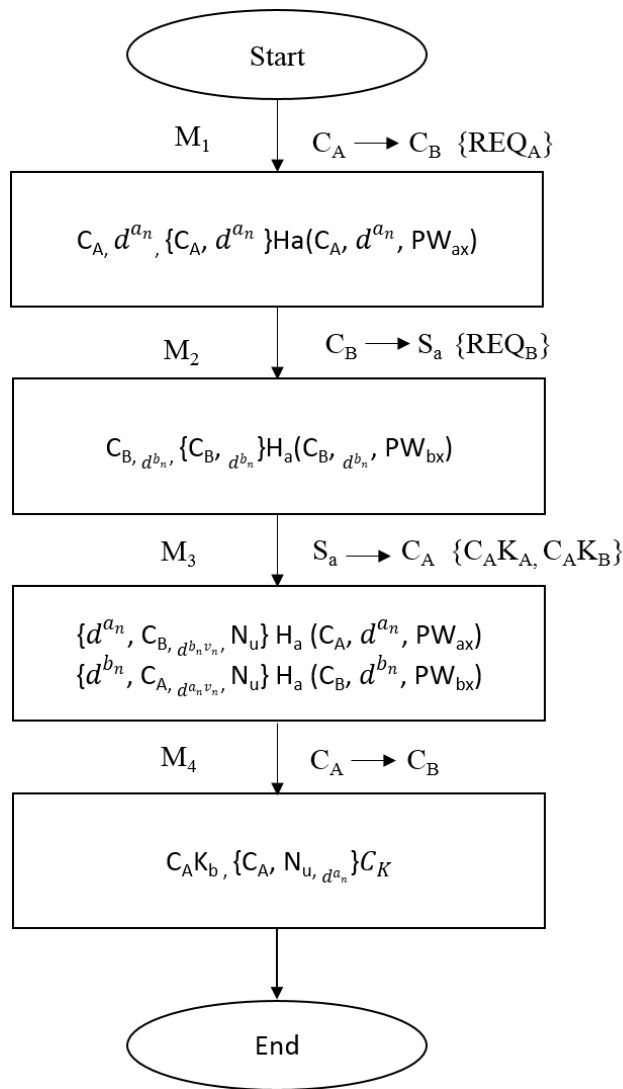
Stage 4: The CA decodes CAKa, then gets the  $d^{a_n v_n}$  as well as Nu assesses, and the  $\text{CK} = (d^{b_n v_n})^{a_n} = d^{a_n b_n v_n}$ , later receives  $\{\text{CA}, \text{Nu}, d^{a_n}\} C_K$ , as well as translate the CAKb,  $\{\text{CA}, \text{Nu}, d^{a_n}\} C_K$  towards the user CB.

Stage 5: Through receiving the CAKb,  $\{\text{CA}, \text{Nu}, d^{a_n}\} K$ , originally then the user CB decodes the code CAKb for obtaining the  $d^{a_n v_n}$  as well as, later validate  $d^{b_n}$ , additionally, CB assesses the  $C_K = (d^{a_n v_n})^{b_n} = d^{a_n b_n v_n}$  as well as later decodes the  $\{\text{CA}, \text{Nu}, d^{a_n}\} C_K$  for authenticating the Nu immediately.

Stage 6: Lastly, both the chosen client CA along the client CB recognize another new session passcode i.e.,  $C_K$  to furthermore chat and then get rid of the probabilities of real-time records of fatalities within the social network model's communication procedure.

This enhanced 3PAKE protocol's entire process is summed up simply by following. Through sending separate identification invites to REQA and REQB but also receiving responses CAKa as well as CAKb, each user CA and user CB may each verify this host Sa. Then, using  $d^{a_n}$  as well as Nu, both clients CA and user CB verify one another's names. Data despatcher uniqueness for the patron CA, as well as patron CB, seems to be present throughout all transmitted data. In addition to giving preference to the individual users through authorized server Sa this same needed confidentiality while conversation through public networking, precise user identification is given top emphasis. Any customer receives a different passcode throughout the conversation that also is encoded inside the dispersed data and gets transmitted across the network, in this manner of distributed messaging through an authorized host to give each user the

necessary anonymity. Although this method jointly verifies both user CA as well as CB in addition to the authorized host Sa, it seems highly resistant to varied assaults including brute force, along with multiple parallel assaults, and man-in-the-middle assaults in real-time.



**Figure 5.4: Depicts flow chart of hash function and symmetric encryption based on improved 3PAKE protocol.**

### 5.5. Protocol 2- Design

Nowadays, maintaining the confidentiality of the transmitting data, which includes audio(s)/video(s) or textual messaging in real-time. The communication among multiple third persons over the server has also become a significant issue. Precise customer authentication has become essential in social network model settings. Network safety becomes a crucial factor in securing private content as required inside the current society. To give necessary anonymity to multiple users when interacting

with one another through the servers, several types of confidentiality protocols have been investigated and implemented in past years.

In modern communication infrastructure, the 3PAKE protocol continues to advance and facilitates the user throughout real-time data transmission. However, there are multiple problems with the current communication standards which relate to the network bandwidth, etc. This privacy-preserving 3PAKE algorithm offers higher security against numerous strikes, such as cryptanalysis assaults replay attacks, and man-in-the-middle attacks in client communication. This research proposed an enhanced 3PAKE protocol for social network secrecy verification to address the shortcomings of contemporary methods.

**Table 5.2: Shows abbreviations used in improvised 3PAKE protocol.**

| S. No | Notions Utilized | Definition                |
|-------|------------------|---------------------------|
| 1     | $CL_A$           | Client                    |
| 2     | $CL_B$           | Client                    |
| 3     | $SR_A$           | Authentic Server          |
| 4     | $dP_A/V_A$       | Private Secret Code Words |
| 5     | $dP_B/V_B$       | Private Secret Code Words |
| 6     | $rp_A$           | Integer                   |
| 7     | $rp_B$           | Integer                   |
| 8     | $InDP_A$         | Request                   |
| 9     | $InDP_B$         | Response                  |

To safeguard the exchanged content amongst multiple clients via the internet, there have been used modified 3PAKE protocol based on two separate techniques namely ECC and SE. This technique is more robust against the different attacks and less complex. This enhanced 3PAKE technique for social network safety validation was designed in two distinct phases, the first one was computer startup and the next one was authenticated credentials exchange. There has been chosen user  $CL_A$ , and user  $CL_B$ , along with the one authenticated server namely  $SR_A$  for the validation of the modified 3PAKE technique. Several key ideas used in this improved 3PAKE technique for the

confidentiality validation of the social network model with a greater accuracy level are represented in Table 5.2.

## 5.6. Protocol 2- System initialization

The multiple rounds of the proposed 3PAKE protocols have been described in this section. Further, the details explanation of the empirical findings, and interpretations are explained thoroughly. The authentic sever SRA initializes and selects specific settings, which include the frequency of users communicating via the genuine site. These two users, CLA and CLB, sign up with this same authenticated host SRA. The network parameters are described as follows:  $Sr2 = St2 + Spt + Sq$  (module  $s$ ), whereby  $p, q \in \mathbb{F}_s$  but also  $5Sp^3 + 28 Sq^2 \neq 0$ . This limited domain, i.e.,  $\mathbb{F}_s$  upon huge integer  $s$ , in addition to the ECC group via this same  $Sp$  points  $QS$  onto curved  $ESs$  ( $Sp, Sq$ ) (module  $s$ ).

For this registration phase, the user CLA and secondary user CLB make a registration over the authenticated server which is denoted by the SRA to create multiple users along with a plurality of private secured passcode pairs, for instance,  $dPA/VA$  along with the  $dPB/VB$ , whereby this  $VA = dPAQ, VB = dPBQ$ , and  $dPA, dPB \in \mathbb{Z}P_n^*$ . Authenticated server SRA chooses multiple isolated passcode  $dPs \in \mathbb{Z}P_n^*$ , along with evaluating these public passcode  $UPs = dPsQS$ . These authenticated passcode interchange phases are depicted as described below.

### 5.6.1. Round 1

This improvised 3PAKE protocol executes in multiple rounds to provide the required safety for multiple confidential datasets translated over social networks in real-time. In this round, the user  $CL_A$  translates a request  $InDP_A$  to another user  $CL_B$  for the request accepted using the secured passcode, thereby aiding in securing the confidential datasets more accurately in real-time, in comparison to the existing approaches. Figure 5.5 illustrates the first round of the improvised 3PAKE protocol.

$$\begin{array}{l}
\mathbf{Round 1} \text{ } CL_A \rightarrow CL_B \quad \{\text{InDP}_A, \text{Request}\} \\
A: \quad \quad \quad rp_A \in ZP_n^*, wp_A \in ZP_q^* \\
\quad \quad \quad RP_A = rp_A V_A, \widehat{RP}_A = rp_A V_S \\
\quad \quad \quad KP_A = dP_{A, \widehat{RP}_A} = kP_{At}, kP_{Ar} \\
\quad \quad \quad WP_{AX} = wP_A QS, CP_A = EP_{At}(RP_A, \\
\quad \quad \quad \quad \quad \quad WP_{AX}) \\
\quad \quad \quad CL_A \rightarrow SR_A \\
\quad \quad \quad \{\text{InDP}_A, \text{InDP}_B, CP_A, RP_A\}
\end{array}$$

**Figure 5.5: Illustrates the first round of the improvised 3PAKE protocol.**

### 5.6.2. Round 2

In this round the user  $CL_B$  translates a request  $\text{InDP}_B$  to another individual  $CL_B$  for the request accepted using the safe passcode, thus aiding in verification and securing the confidential records in a more pragmatic and secured manner, while making a comparison with existing approaches. Figure 5.6 illustrates the second round of the improvised 3PAKE protocol.

$$\begin{array}{l}
\mathbf{Round 2} \text{ } CL_B \rightarrow CL_A \quad \{\text{InDP}_B, \text{Response}\} \\
B: \quad \quad \quad rp_B \in ZP_n^*, wp_B \in ZP_q^* \\
\quad \quad \quad RP_B = rp_B V_B, \widehat{RP}_B = rp_B V_S \\
\quad \quad \quad KP_B = dP_{B, \widehat{RP}_B} = kP_{Bt}, kP_{Br} \\
\quad \quad \quad WP_{BX} = wP_B QS, CP_B = EP_{Bt}(RP_B, \\
\quad \quad \quad \quad \quad \quad WP_{BX}) \\
\quad \quad \quad CL_B \rightarrow SR_A \quad \{\text{InDP}_B, \text{InDP}_A, CP_B, RP_B\}
\end{array}$$

**Figure 5.6: Illustrates the second round of the improvised 3PAKE protocol.**

### 5.6.3. Round 3

In this round, the authorized server performs validation of both the user and effectively checks, the received  $RP_A$ , as well as  $RP_B$ , in real-time records translation and exchange amongst the users. Figure 5.7 illustrates the third round of the improvised 3PAKE protocol.

|   |
|---|
| <p><b>Round 3</b> <math>SR_A</math>: <math>KP_A = dP_S RP_A = (kP_{At}, kP_{Ar})</math></p> <p><math>KP_B = dP_S RP_B = (kP_{gt}, kP_{Br})</math></p> <p><math>(RP_A, WP_A) = DP_{AK} (CP_A)</math></p> <p><math>(RP_B, WP_B) = DP_{BK} (CP_B)</math></p> <p>Checked: Obtained <math>RP_A=?</math> Decrypted <math>RP_A</math></p> <p>Checked: Obtained <math>RP_B=?</math> Decrypted <math>RP_B</math></p> |
|---|

**Figure 5.7: Illustrates the third round of the improvised 3PAKE protocol.**

#### 5.6.4. Protocol 2- Safe code exchange stage of enhanced 3PAKE protocol

In this improvised 3PAKE technique designing, the key three essential entities are, the server defined through the SRA, authorized user CLA, and authorized user CLB, which have been defined in this enhanced 3PAKE approach for secrecy validation of social network. This authorized party CLA, and authorized party CLB, seek to construct a secure connection secret code for one another to verify the enhanced privacy checking methodology. This trustworthy server was used for authentic interaction across the global connection to transmit the secured transaction secret code. This verification procedure has been carried out through multiple distinct steps, which are explained below.

Stage 1. It's one of the beginning stages of the improvised 3PAKE technique. Herein, this valid party CLA performs a specified round.

Phase 1: Further, choose the numeral to initialize i.e.,  $rp_A \in ZP_n^*$  randomly and afterward that execute  $CHA = CH (CRA || CDA)$  and  $CRA = CHA . CQ$ .

Phase 2: Next, assess  $CKA = CDA . CUS = CDA . CDS . CQ$  as well as  $KCAS = CH (CIDA || CIDB || CRA || CKA)$ .

Phase 3: The translation of  $(CIDA, appeal)$  as well as  $(CIDA, CIDB, CRA, KCAS)$  towards the authentic patron CLB along with authentic main-server SRA, correspondingly.

Stage 2. Once this authentic patron CLA efficaciously sends the beginning communication datasets package  $(CIDA, appeal)$ , later this authentic patron CLB performs the following phases illustrated below.



Phase 1. Choose the numeral to initialize i.e.,  $rp_B \in ZP_n^*$  randomly as well as afterward which assesses the  $CHB = CH (CRB||CDB)$  as well as  $CRB = CHB. CQ$ .

Phase 2: Assess this  $CKB = CDB. CUS = CDB. CDS. CQ$  as well as  $KCBS = CH (CIDB || CIDA || CRB || CKB)$ .

Phase 3: Transfer this  $(CIDB, appeal)$  and this  $(CIDB, CIDA, CRB, KCBS)$  towards this authentic patron CLA along with authentic main-server SRA, correspondingly.

Stage 3. Whereas gaining this  $(CIDA, CIDB, CRA, KCAS)$  and  $(CIDB, CIDA, CRB, KCBS)$  through genuine patron CLA, as well as authentic patron CLB, afterward which this genuine main-server SRA performs these implicit processes.

Phase 1: Next, regulate symmetrical passcode for verification  $CKA = CdS. CUA = CdA. CdS. CQ$  as well as  $CKB = CdS. CUB = CdB. CdS. CQ$ , correspondingly.

Phase 2: Furthermore, assess this  $\overline{KC}_{AS} = CH (CIDA || CIDB || CRA || CKA)$  using this obtained CRA and assessed CKA. CS regulate state  $\overline{KC}_{AS} = ? KC_{AS}$ . Although it is not encountered, at that moment the authentic main-server SRA renders the confirmation ineffective notice towards the authentic patron CLB or authentic main-server SRA assesses the  $KC_{AS} = CH (CIDA || CIDB || CRA || CKA)$  as well as decodes the notice  $(CRB, KCSA)$  to authentic patron CLA.

Phase 3: Evaluate this  $\overline{KC}_{BS} = CH (CIDB || CIDA || CRB || CKB)$  using attained CRB but also assessed CKB. CS fix state  $\overline{KC}_{BS} = ? KC_{BS}$ . Whereas it met, afterward authentic main-server SRB decodes this confirmation failed message towards the authentic patron CLA or authentic main-server SRB assesses this  $KC_{BS} = CH (CIDB || CIDA || CRB || CRB || CKA)$  and decodes this packet  $(CRA, KCSB)$  towards authentic patron CLB.

Phase 4: Through gaining this  $(CRB, KCSA)$ , the main authentic patron CLA assesses this  $\overline{KC}_{AS} = CH (CIDA || CIDB || CRA || CKA)$  applying this own CRA with CKA created within stage 1 and this obtained CRB. Afterward, this authentic patron CLA confirms this state  $\overline{KC}_{AS} = ? KC_{AS}$ . Although this consequence arises constructive, later this authentic patron CLA assesses meeting passcode  $CSK = CH (CIDA || CIDB || CRA || CKB || CK)$ , whereas this  $CK = CHA. CRB = CHA. CHB. CQ$ , or else in additional situations this authentic patron CLA rejects this enhanced protocol.

Afterward, this authentic patron CLB accomplishes this subsequent procedure and later, gets this notice (CRB, KCSB) via the authentic main-server SRA.

Phase 5: Through receiving this (CRA, KCSB), the main authentic patron CLB assesses this  $\overline{KC}_{BS} = CH (CIDB \parallel CIDA \parallel CRB \parallel CKB)$  applying this CRB along with the CKB created within phase 2 and this obtained CRA. Further, this authentic patron CLB confirms this state  $\overline{KC}_{BS} = ? KC_{BS}$ . Whenever this consequence arises expectant, afterwards authentic patron CLB assesses meeting passcodes  $CSK = CH (CIDA \parallel CIDB \parallel CRA \parallel CKB \parallel CK)$ , whereas this  $CK = CHB$ .  $CRA = CHA$ .  $CHB$ .  $CQ$ , then in additional situations this authentic patron CLB rejects this anticipated procedure within the real-time implementation over key public networks.

### 5.7. Summary

In this thesis work, multiple enhanced 3PAKE protocols have been implemented in the AVISPA tool for security verification of the social network model. Protocol-1 is developed for enhanced 3PAKE protocol design. In this protocol key notions used are as follows: CA and CB are to distinct clients and Sa is the authenticated server. This protocol is rooted in the DHKE approach and a combination of HF and SE. The symmetric key exchanged between CA and Sa is  $PW_{bx}$  and the symmetric key interchanged between CB and Sa is denoted by  $PW_{bx}$ . This 3PAKE protocol is designed in six distinct stages which include distinct messages denoted by  $M_1$  to  $M_4$  as denoted in Figure 5.4. Protocol 2 of the 3PAKE protocol is developed based on ECC and SE. This was implemented in 2 separate stages. The first was about the computer startup and the next was regarding the authenticated credential interchange. Protocol 2- system initialization is done in 3 rounds and the safe code exchange stage of enhanced 3PAKE based on ECC and SE was done in six separate phases.

## CHAPTER 6 RESULTS AND DISCUSSION

In this research, an innovative and modified social network model has been developed which is rooted in the multiple enhanced 3PAKE protocols for social network dataset's privacy and confidentiality in comparison to existing work. The developed protocols are based on diverse techniques i.e., the first enhanced protocol is mainly rooted in the HF and SE, whereas the second protocol is rooted in the SE as well as ECC. Both protocols offer improved performance constraints such as parse time, as well as searching period, depth plies, and multiple visiting nodes in real-time execution of the protocols. These protocols also give greater secrecy against various assaults like brute force, man in the middle, etc.

This research's main contributions include the validation of an enhanced and innovative 3PAKE protocols-based framework with a reduced running period, reduced processing burden, resistance to a variety of assaults, and excellent transmission efficiency in a practical way. The conventional protocols have some drawbacks related to the confidentiality of data in the modern world against multiple threats including man-in-the-middle, replay attacks, etc. Moreover, numerous investigators have worked pragmatically to create numerous confidentiality procedures over the previous years for offering this desired confidentiality to the patrons during the interaction. To address such a problem, there have been proposed multiple unique 3PAKE protocols-based combined frameworks, which are rooted in these protocols. The framework is based on HF, and SE, along with the ECC, and SE approaches, respectively. These protocols use very minimal execution time in protocol execution. Furthermore, the suggested approach is capable of managing complex communication through social networks while providing increased privacy.

### **6.1. Protocol 1- Improvised 3PAKE specifications**

In this research, the AVISPA software package was used to validate the enhanced 3PAKE protocol. The outcome of the proposed 3PAKE protocol demonstrates that the suggested protocol is more secure and provides a high level of

data secrecy in social network settings against multifarious attacks. Three fundamental functions in enhanced 3PAKE protocols architecture are specified in the HLPSL syntax, which includes  $pekc\_CA$ ,  $pekc\_CB$ , and  $pekc\_Sa$ , which stands for the patron CA, CB, and authorized server Sa, correspondingly. Therefore, this offers one single key role, Sa, as seen in Figure 6.1. The authorized host Sa waits again for client CB to submit this same REQB as well as REQA before sending this same CAKA as well as CAKB to CA. Sa would change from 0 to 1 within the same iteration phase St of this authorized host. In this fundamental role, Sa uses a few characters that are detailed in Table 6.1.

**Table 6.1: Illustrates the symbols used in the Sa role.**

| S. No. | Symbols            | Meaning of the used symbol           |
|--------|--------------------|--------------------------------------|
| 1      | Hash (.)           | Represents hash function             |
| 2      | Snd (M)            | Forward message                      |
| 3      | $C_A$              | Identity of the first user           |
| 4      | $C_B$              | Identity of the second user          |
| 5      | $S_a$              | Authenticated server                 |
| 6      | $PW_{ax}, PW_{bx}$ | Represents symmetric keys used       |
| 7      | Rcv (M)            | Represents obtained message M        |
| 8      | new ()             | Originate an arbitrary no. used once |

## 6.2. Protocol 1- Improvised 3PAKE secrecy evaluation

Firstly, this authentic main-server Sa receives a beginning message that is  $(CB. Gy'.\{CB. Gy'.Nb'\}_{Hash} (CB. Gy'. PW_{bx}). CA. Gx'.\{CA. Gx'\}_{Hash} (CA. Gx'. PW_{ax})$  via Rcv () function. Furthermore, the authentic main-server Sa chooses any own randomized numeral Nz' but also assesses this Gxz'. Finally, authentic server Sa translates the message  $\{Gx'.CB. Gyz'. Nb'\}_{Hash} (CA.Gx'.PW_{ax}). \{Gy'.CA. Gxz'\}_{Hash} (CB. Gy'. PW_{bx})$  via Snd () function. For secrecy verification, the DHKE approach for this improvised 3PAKE protocol design is based on HF and SE for social network secrecy and confidentiality. After defining fundamental key roles, there is one obligation to describe the collected role which describes the fresh meeting codes for the enhanced 3PAKE procedure. Figure 6.1 depicts the key role of this authentic main-server Sa for this recommended 3PAKE technique regarding the required secrecy of the social networking verification. Figure 6.2 depicts another role which is a session role of the enhanced 3PAKE protocol secrecy verification of social networks.

### **6.3. Protocol 1- Informal secrecy evaluation**

Each fundamental function, including the  $pekc_{CA}$ ,  $pekc_{CB}$ , as well as  $pekc_{Sa}$ , has been explored using clear rationale throughout various transaction parts. In the protocol execution process, a higher-level parametric setting is required for performance evaluation. Every environmental role includes a configuration of a single or more encounters in addition to common variables. The environmental role impact of this enhanced 3PAKE technique for privacy assurance of social networking sites is shown in Figure 6.3. Thus, 1 is used to symbolize the intrusive party which utilizes a strong connection to execute the recommended 3PAKE technique to determine man-in-the-middle, replay, and cryptanalysis assaults.

Furthermore, the channels (dy) represent this Dolev-Yao paradigm, which is the prototype invader. Through using this architecture, the intrusive party has complete command throughout the network, ensuring that each communication transmitted through users goes through the intrusive assessment. While the server retrieves the necessary keys, the intrusive verification is examined for precise verification of user credentials. As a consequence, subscribers may send and get information, using whatever path they want to establish over the accessible communication channel based on priority and availability.

```

role pekc_Sa (CA, CB, Sa      : agent
             Snd, Rcv        : channel (dy),
             PWax, PWbx     : symmetric_key,
             G                : text,
             Hash            : hash_func)
Played_by S def=
  local St      : nat,
  Nz           : text,
  Nb           : text,
  Gx, Gy      : message,
  Gyz, Gxz    : message
  init St := 0
  transition
  St = 0 /\ Rcv (CB. Gy'.{CB. Gy'.Nb'}
             _Hash (CB. Gy'. PWbx). CA.Gx'.
             {CA. Gx'}_Hash (CA. Gx'. PWax)) = |>
  St' := 1 /\ Nz' := new()
             /\ Gxz' := exp (Gx', Nz')
             /\ Gyz' := exp (Gy', Nz')
             /\ Snd ({Gx'.CB. Gyz'. Nb'}
                    _Hash (CA.Gx'. PWax).
                    {Gy'. CA. Gxz'}_Hash(CB. Gy'. PWbx))
             /\ witness (Sa, CA, auth_a_s_gx, Gx')
             /\ witness (Sa, CB, auth_b_s_gy, Gy')
end role

```

**Figure 6.1: Depicts authentic main server  $S_a$  role for verification.**

```

role session (CA, CB, Sa      : agent
             PWax', PWbx'   : symmetric_key,
             G               : text,
             Hash            : hash_func)
def=
  local CA_SND, CA_RCV, CB_SND, Sa_SND, Sa_RCV: channel (dy)
  composition
  pekc_CA (CA, CB, Sa, CA_SND, CA_RCV, PWax', G, Hash)
  /\ pekc_CB (CA, CB, Sa, CB_SND, CB_RCV, PWbx', G, Hash)
  /\ pekc_Sa (CA, CB, Sa, Sa_SND, Sa_RCV, PWax', PWbx', G, Hash)
end role

```

**Figure 6.2: Depicts session role for verification of enhanced 3PAKE.**

```

role environment ()
def=
  const
    a, b, s, i          : agent
    PWax, PWbx, PWi    : symmetric_key,
    d                  : text,
    hash               : hash_func,
    auth_a_b_nb       : protocol_id,
    auth_b_a_dx       : protocol_id,
    auth_a_s_gx       : protocol_id,
    auth_b_s_gy       : protocol_id,
    sec_a_b_gxyz      : protocol_id,
    intruder_knowledge = {i, a, b, s, pwi, g, hash}
  composition
    session (a, b, s, PWax, PWbx, g, hhash)
  /\ session (a, b, s, PWax, PWbx, g, hhash)
  /\ session (i, b, s, PWi, PWbx, g, hhash)
  /\ session (a, i, s, PWax, PWi, g, hhash)
end role

```

**Figure 6.3: Depicts environmental role for verification of enhanced 3PAKE.**

The analytical objective of the proposed enhanced 3PAKE technique for the social network confidentiality validation is shown in Figure 6.4. Numerous metrics listed below have been examined that are taken into account in the analysis goal. This sign denotes that the participant's CA verifies Sa across gx.

```

goal
  authentication on auth_CA_SA_gx
  authentication on auth_CB_SA_gy
  authentication on auth_CA_SB_nb
  authentication on auth_CB_SA_gx
  secrecy_of sec_a_b_gxyz
end goal

```

**Figure 6.4: Depicts analysis goal for verification of enhanced 3PAKE.**

Throughout the background, several 3PAKE techniques have been explored to produce a safe communication code amongst customers while utilizing a reliable host. Conventional adapted 3PAKE methods, nevertheless, suffer from several shortcomings and therefore are incapable of providing essential secrecy in social network sites against multiple attacks namely man-in-the-middle, cryptanalysis, etc. This proposed enhanced 3PAKE protocol is implemented using the personal computer (PC). The PC

configuration details are as follows: Operating System (OS) of 64-bit, processor: intel i7, RAM of 16GB, and the installed window was 10. The simulation of the proposed 3PAKE protocol is performed using the AVISPA software package.

#### **6.4. Protocol 1- Performance computation**

Figure 6.5 shows simulated results obtained using the OFMC-based backs-end for the proposed enhanced 3PAKE technique for secrecy validation of the social network model. The comparative analysis of the enhanced 3PAKE technique with state-of-the-art techniques is shown in Table 5.2. Islam and colleague's [102] approach requires 0.00s for parseTime, 5.0 steps for connectivity, 0.660s for searching, 6 steps for depths, and 16 steps for visiting sites. Whereas the protocol developed by Pak and colleagues [103] requires a parse duration of 0.000 seconds, transmission stages of 5, searching duration of 8.940 seconds, depths plies 6.0, and 1690 visited sites.

This enhanced 3PAKE protocol gives a parsing period of 0.000 seconds, search time of 0.120 seconds, depth of 4.0 plies, visiting nodes of 10, and interaction stages of 2, which demonstrate that each variable has been lowered from the previous methods. As a result, our proposed 3PAKE protocol promises extremely low computation intricacy together with a shortened selection moment for the client's verification through the authentic server  $S_a$ . This parsing period provides data about the initiation timing of protocol processing for the users and host verification. To efficiently record actual search times for the users and authorized servers, it must be originally fixed to 0.000 milliseconds. Additionally, the enhanced method is better resistant to a variety of attacks, such as man-in-the-middle, cryptanalysis attacks, etc. The proposed 3PAKE protocol offers high security in social network settings. The password patterns have been created utilizing identical longer-term encoding elements during the subsequent cycle. Elements  $a_n$ ,  $b_n$ ,  $a_s$ , and  $v_n$  within this recommended 3PAKE technique, are all randomly selected and self-governed to the recommended 3PAKE protocol implementation. Therefore, the previous access passwords were unable to be revealed by the leaked confidential passwords  $PW_{ax}$ ,  $PW_{bx}$ , or  $CK$ . Table 6.2 depicts enhanced 3PAKE protocol results for the social network model.



```

SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/avispa/web-interface-
computation/./tempdir/workfileEdDMf1/3PAKE.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.12s
  visitedNodes: 10 Nodes
  depth 4 plies

```

**Figure 6.5: Depicts simulated results through the OFMC back-ends.**

**Table 6.2: Depicts enhanced 3PAKE protocol results for the social networking model.**

| S. No. | Protocols                   | parseTime | Communication steps | searchTime | Depth (plies) | Visited Nodes |
|--------|-----------------------------|-----------|---------------------|------------|---------------|---------------|
| 1      | S. K. H. Islam et al. [102] | 0.00s     | 5                   | 0.66s      | 6             | 16            |
| 2      | K. Pak et al. [103]         | 0.00      | 5                   | 8.94s      | 6             | 1690          |
| 3      | Proposed 3PAKE protocol     | 0.00      | 2                   | 0.12s      | 4             | 10            |

### 6.5. Protocol 2- Performance analysis

This study was carried out using the latest well-known simulation software, AVISPA. To give the necessary concealment to the clients throughout real interaction across open social networks in an even sufficiently secured way, as requested in the current transmission architecture. This research presented an enhanced 3PAKE protocol to offer high security to confidential information in social network settings.

### 6.5.1. Protocol 2- Specifications

Due to the rapid expansion of consumers across constrained connections and the frequent technical breakthroughs in the transmission field today multiple communication protocols are changing continuously. As a result, a novel confidentiality technique must be created that enables safe transmission and minimizes the possibility of data leakage when using shared connections. Moreover, a unique 3PAKE secrecy protocol is implemented which is based on SE and ECC approach to address the security breach issues by different attacks on the network.

### 6.5.2. Protocol 2- Security evaluation and validation

The widely used AVISPA software was installed in a PC system having the accompanying platform settings to verify the confidentiality of the enhanced 3PAKE framework. The main configuration of the system is as follows: RAM:16 GB, processor: Intel-i3-1005G1 clocked at 1.200 GHz, 64-bit OS. AVISPA tool is built using a role-rooted language. It suggests that each participant does have a defined task to execute the protocol. Each procedure is independent, getting initial input from attributes and communicating with other functions using credentials. It is essential to track the communication link continuously in the communication procedure. The execution of the enhanced 3PAKE method enables confidentiality certification of the social network in real interaction via an authorized host. Table 6.3 displays the symbols used throughout different roles including session, environment, and objective.

**Table 6.3: Illustrates chosen symbols in multiple roles of improvised 3PAKE.**

| S. No | Symbol | Meaning/Definition of the specified symbols |
|-------|--------|---|
| 1     | $CL_A$ | Authenticated Client                        |
| 2     | $CL_B$ | Authenticated Client                        |
| 3     | $SR_A$ | Authenticated Server                        |
| 4     | subs1  | Protocol ID                                 |
| 5     | subs2  | Protocol ID                                 |
| 6     | subs3  | Protocol ID                                 |
| 7     | new () | Generate a random no. utilized one time     |

```

role alex (CLA, SRA, CLB : agent),
% CH is hash function
CH, Mul: hash_func, Snd, Rcv: channel (dy))
Played_by CLA
Def =
local State : nat,
DCLA, UCLA, IDCLA, IDCLB, CRCLA, CQ, CUS: text,
HCLA, RCLA, RCLB, KCLA, CCLASRA, CSRAKCLA : message,
Inc : hash_func
const alex_server, server_max, alex_max, alex_server,
Subs1, subs2, subs3 : protocol_id
Init State :=0
transition
1. State = 0 ∧ Rcv (start) = |>
State' := 1 ∧ DCLA' := new ()
∧ UCLA' := Mul (DCLA' . CQ)
∧ RACLA' := new ()
∧ HCLA' := CH (RCLA' . DCLA')
∧ RCLA' := Mul (HCLA' . CQ)
∧ KCLA' := Mul (DCLA' . USRA)
∧ CCLASRA' := CH (CIDCLA' . CIDCLB' . CRA' . KCLA')
∧ Snd (CIDCLA' . CIDCLB' . CRCLA' . KCLA')
∧ Secret ({CDCLA'}, subs1, {CLA, SRA})
2. State = 1 ∧ Rcv (RCLB' . CSRA') = |>
State' := 2 ∧ CK' := Mul (CHCLA' . RCLB')
∧ SRAKCLA' := CH (CIDCLA' . CIDCLB' . RCLA' . RCLB' . K')
End role

```

**Figure 6.6: Depicts stated role for authentic main client CLA.**

The HLPSL simulator's designated function for the verified user CLA is shown in Figure 6.6. Several primary elements used to construct the enhanced 3PAKE approach are defined thoroughly. Thus, the selected sign SRA stands for the authorized site, while CLA, and CLB, symbolize the authorized customers that desire to connect through the server.

```

role max (CLB, SRA, CLA : agent),
% CH is hash function
CH, Mul: hash_func, Snd, Rcv: channel (dy))
Played_by CLB
Def =
local State : nat,
DCLB, UCLB, IDCLB, IDCLB, CRCLB, CQ, CUS: text,
HCLB, RCLB, RCLA, KCLB, CCLBSRB, CSRBKCLB : message,
Inc : hash_func
const alex_server, server_max, alex_max, alex_server,
Subs1, subs2, subs3 : protocol_id
Init State :=0
transition
1. State = 0 ∧ Rcv (start) = |>
State' := 1 ∧ DCLB' := new ()
∧ UCLB' := Mul (DCLB'. CQ)
∧ RACLB' := new ()
∧ HCLB' := CH (RCLB'. DCLB')
∧ RCLB' := Mul (HCLB'. CQ)
∧ KCLB' := Mul (DCLB. USRB)
∧ CCLBSRB' := CH (CIDCLB. CIDCLA. CRB'. KCLB')
∧ Snd (CIDCLB. CIDCLA. CRCLB'. KCLB')
∧ Secret ({CDCLB'}, subs1, {CLB, SRB})
2. State = 1 ∧ Rcv (RCLA. CSRB') = |>
State' := 2 ∧ CK' := Mul (CHCLB. RCLA)
∧ SRAKCLB' := CH (CIDCLA. CIDCLB. RCLA. RCLB. K')
End role

```

**Figure 6.7: Depicts stated role for authentic main client CL<sub>B</sub>.**

```

role server SRA (SRA, CLA, CLB : agent,
% CH is hash function
CH, Mul: hash_func,
Snd, Rcv: channel (dy))
played_by SRA
Def =
local State : nat,
DSRA, UCLB, UCL_A, IDCL_A, IDCL_B, CRCL_B, CQ, CUSRA: text,
HCLB, RCLB, RCL_A, SRAKCLB, CCLB_SRA, CSRAKCLB : message,
Inc : hash_func
const alex_server, server_max, alex_max, alex_server,
Subs1, subs2, subs3 : protocol_id
Init State :=0
transition
1. State = 0  $\wedge$  Rcv (CIDCL_A. CIDCL_B. CRCL_A'. CKCL_A') Rcv (CIDCL_A.
CIDCL_B. CRCL_B'. CK.CLB')
State' := 1  $\wedge$  CUSRA' := Mul (DSRA'. CQ)
 $\wedge$  CKCL_ACL_A' := Mul (DAR_A'. UCL_A)
 $\wedge$  CKCL_BCL_B' := Mul (DAR_A'. UCL_B)
 $\wedge$  CSRACL_A' := CH (CIDCL_A. CIDCL_B. CR_A . CR_B'. CKCL_ACL_A')
 $\wedge$  CSRACL_B' := CH (CIDCL_B. CIDCL_A. CR_B . CR_A'. CKCL_BCL_B')
 $\wedge$  Snd (CRCL_B. CRSRACL_A')
 $\wedge$  Snd (CRCL_A. CRSRACL_B')
 $\wedge$  Secret ({CDSRA'}, subs3, {SRA})
End role

```

**Figure 6.8: Depicts the stated role of authentic main server SRA.**

The authorized user CLB designated function inside the HLPSL simulations is depicted in Figure 6.7. The HLPSL simulator defined function for the authorized client SRA is shown in Figure 6.8. There have been selected multiple procedure IDs, notably subs1, subs2, and subs3 to accurately confirm the enhanced 3PAKE protocol against multiple assaults, which includes man-in-the-middle, cryptanalysis threats to provide added security towards the client's private data over social connections. When the enhanced 3PAKE technique is implemented, a randomized integer generated by function initial () is used once.

### 6.5.3. Informal security assessment

The user builds a unique session password using credentials exchanging procedures that offer important cryptographic-based approaches that could be used to secure communication in shaky broadcasting channels. Efficient client authentication becomes crucial to prevent unauthorized consumers from accessing information and resources due to the fast advancement of connectivity and digital technologies. Through sharing secured session keys and creating an encryption link through an authorized host,

the 3PAKE protocol allows numerous clients to interact safely over insecure connections.

```

role session (CLB, SRA, CLA : agent),
CH, Mul: hash_func),
def =
local CSI, CSJ, CRI, CRJ, CTI, CTJ: channel (dy)
composition
Alex (CLA, SRA, CLB, CH, Mul, CSI, CRI)
Server (CLA, SRA, CLB, CH, Mul, CSJ, CRJ)
max (CLA, SRA, CLB, CH, Mul, CTI, CTJ)
End role

```

**Figure 6.9: Depicts the main role of the session.**

Consequently, the user needs to memorize the passcode to recognize verified passcodes over the authentic server in real interaction. The client-server records the credentials, which are to be calculated across the legitimate passcode. Again, to validate the enhanced 3PAKE protocol, invader had been shown would provide an effective way to use the DolevYao technique. This role framework offers a way to describe the various meetings, which may include several concepts in addition to various types of responsibilities, for instance, the environmental role inside the real-time implementation of the protocols. This designated position for such sessions inside the HLPSL simulation is shown in Figure 6.9. Each environment's designated function inside the HLPSL simulator is shown in Figure 6.10. Each goal's designated function inside the HLPSL simulator is shown in Figure 6.11.

```

role environment
def =
const CLA, SRA, CLB: agent,
Ch, mul: hash_func,
cida, cidb, cua, cub, cda, cdb, cra, crb, sds, us, cas, cbs, csa, csb,
kka, kkb, ha, hb, ka, kb, raa, rbb: text,
alex_server, server_max, alex_max, alex_server,
subs1, subs2, subs3 : protocol_id
intruder_knowledge = {a, s, b, h, mul, csa, csb, cas, cbs, ra, rb}
composition
session (a, s, b, h, mul)
 $\wedge$  session (s, a, b, h, mul)
 $\wedge$  session (b, s, a, h, mul)
End role

```

**Figure 6.10: Depicts the main role of the environment.**

```
role goal
secrecy_of subs1
secrecy_of subs2
secrecy_of subs3
authentication_on alex_server_raa
authentication_on max_server_raa
End goal
```

**Figure 6.11: Depicts the main role goal of improvised 3PAKE.**

Numerous experts have identified numerous benefits of techniques resembling 3PAKE mostly in the past under the perspective of security. Nevertheless, an additional key benefit of this approach has been acknowledged by numerous experts is that this enhanced 3PAKE approach offers a simple solution for a wide range of client-to-client interaction situations.

```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/avispa/web-interface-
computation/./tempdir/workfileEdDMf1/3PAKE.if
GOAL
as specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.09s
visitedNodes: 20 Nodes
depth 6 plies
```

**Figure 6.12: Depicts the simulated outcomes through the OFMC back-end.**

Additionally, no client has to memorize cryptography keys for additional clients to connect. In particular, using the 3PAKE approach could be applied to several online platforms, including social networks, to safeguard individuals' critical information, which is necessary for the current setting. This uses the widely used AVSIPA application to illustrate the primary effects of both the recommended 3PAKE approach on back-ends OFMC. Figure 6.12 shows the simulated outcomes for both the enhanced

3PAKE confidentiality techniques enabling open networking identification using the OFMC back-end.

**Table 6.4: Shows a comparative analysis of the results of improvised 3PAKE.**

| S. No | Protocols Name         | No. of Total Visited Nodes | searchTime | parseTime | No. of Communication Steps | Depth (in plies) |
|-------|------------------------|----------------------------|------------|-----------|----------------------------|------------------|
| 1     | K. Pak et al. [114]    | 18                         | 7.74s      | 0.00s     | 6                          | 7                |
| 2     | Y. Tang et al. [115]   | 17                         | 0.88       | 0.00s     | 6                          | 5                |
| 3     | Suggested 3PAKE method | 20                         | 0.09s      | 0.00s     | 2                          | 6                |

The verified 3PAKE technique effectiveness evaluation and outcomes for the social networking model confidentiality validation are shown in Table 6.4. The protocol implemented by Pak and colleagues [114] requires parsing timing of 0.000s, depths in plies of 7.0, and the total number of nodes observed 18, containing 6.0 communication stages in real interaction. Tang and colleague's [115] protocol spent the parsing timing 0.000 sec., the total searching duration of authorized users 0.880 sec, depths plies 5.0, and total interaction phase 6.00 and visiting networks 17. The enhanced 3PAKE protocol was found more effective and robust against different attacks namely man-in-the-middle, cryptanalysis assaults, etc. While making a comparison of Pak and colleagues [114] and Tang and colleagues [115] procedure, our implemented protocol provides improved performance and less computational intricacy. The enhanced 3PAKE method requires a search time of 0.090s, parsing timing of 0.000 sec, total communication stages 2.0 during confirmation, depth plies 3.0, and total visiting nodes 20. To avoid the possibility of real-time error, all experimental trials were performed with extreme care and anonymity.

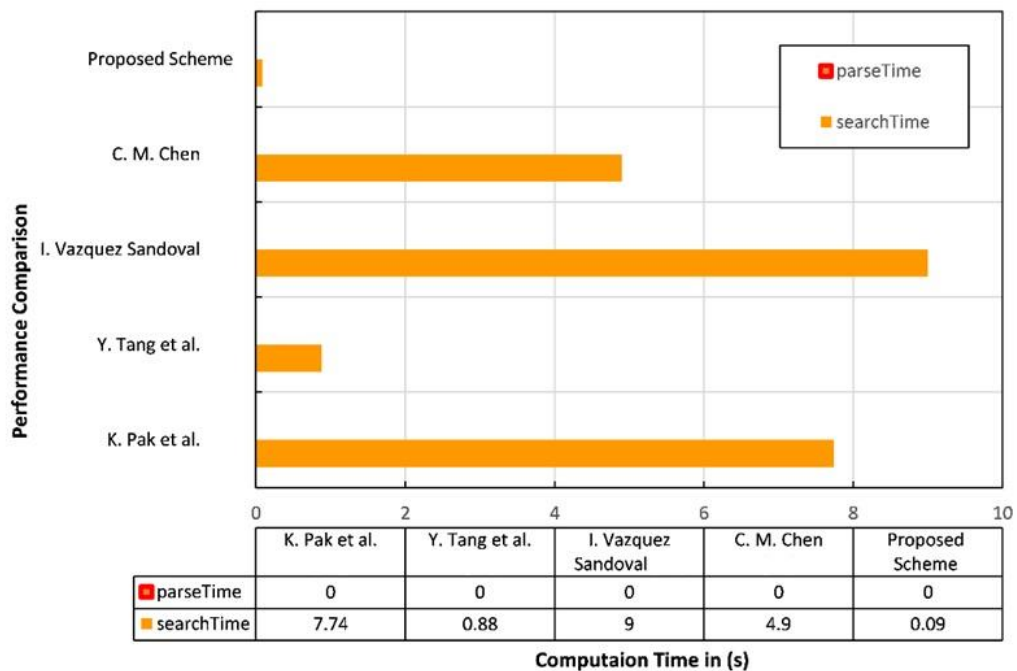
## 6.6. Simulation results

Due to several recognized assaults, such as man-in-the-middle, cryptanalysis, and numerous others, social networking secrecy validation is a challenging task. The biggest intricacy is to keep sensitive credentials and insights very confidential. Although, researchers presented a wide range of network protocols to address the existing vulnerabilities. Despite substantial technical improvements inside the current



connectivity architecture, this risk of information leaking is turning into a serious problem. In this work, there has been implemented an enhanced 3PAKE technique for the validation of social networking models to resolve the abovementioned attacks.

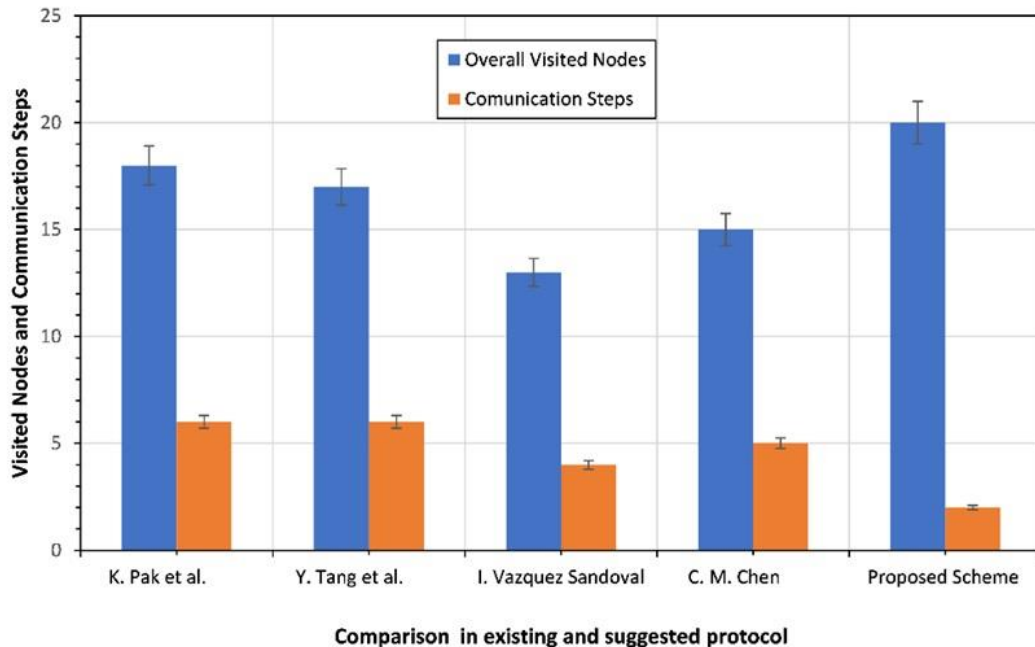
It is found that the enhanced 3PAKE protocol reduces storage complexities, improves computing cost, and streamlines total interaction procedures when compared to the previously developed methods. To correct and validate the session passwords in the proposed enhanced 3PAKE protocol, there are two sets of interaction stages. Furthermore, the proposed 3PAKE protocol is capable of defending against client password leak attacks, and complete server-based-internal attacks, comprising man-in-the-middle attacks, in addition to vulnerability scanning. The suggested 3PAKE protocol provides more privacy and little computing cost. This, allows it to meet all the transmission needs for vast connections along with little throughput.



**Figure 6.13: Depicts the enhanced 3PAKE protocol execution time.**

Figure 6.13 shows the enhanced strategy processing time as well as the various 3PAKE techniques that have been recently identified. Figure 6.13 demonstrates that the proposed 3PAKE protocol consumes much less search time. The enhanced 3PAKE protocol requires 0.09 seconds of searching timing. However, the protocol developed by Pak and colleagues [114], Tang and colleagues [115], Sandoval and colleagues [116], and Chen and colleagues [117], needs 7.740 seconds, 0.880 seconds,

9.0 seconds, and 4.90 seconds, in execution, correspondingly. The state-of-the-art implemented protocols have enormous computing overhead during real deployment because of the long operation duration. As a result, compared to other existing methods, this recommended 3PAKE protocol gives optimal outcomes.



**Figure 6.14: Depicts enhanced 3PAKE protocol communication step and visiting node comparison.**

Figure 6.14 shows the enhanced 3PAKE method of visiting sites, communicating processes, and the numerous state-of-the-art 3PAKE techniques implemented in recent years by different investigators. While comparing the protocol developed by Pak and colleagues [114], Tang and colleagues [115], Sandoval and colleagues [116], as well as Chen and colleagues [117], it is found that the proposed 3PAKE protocol visits above 20.00 nodes. It is also evident from Figure 6.14 when compared to other 3PAKE protocols developed by Pak and colleagues [114], Tang and colleagues [115], Sandoval and colleagues [116], and Chen and colleagues [117], this improvised 3PAKE protocol only requires 2 interaction stages throughout the assessment process. The measured results show that the proposed 3PAKE method offers optimum outcomes and minimal computational complexity.

Due to the rapid development of networks and computing technology, practical client verification is essential to prevent unauthorized users, from accessing operations and a variety of assets. The 3PAKE technology enables two different users to

communicate securely across insecure networks to interchange protected session keys, thereby, establishing a protected path via a trusted host. The patrons store the personal scrutinizer, which is derived with actual true code, in the registry of both the separate trusted sites. There is a need to remember the terms of verification namely the authenticated code with a reliable host. From the safety verification, the improvised 3PAKE protocol offers a wide range of advantages against multifarious network attacks. However, previous investigators recognized existing model advantages which offer a simple technique for user-to-user communication settings and eliminate the need for every customer to remember multiple codes that communicate with one another. The 3PAKE technique can be used in a variety of technological systems in addition to online media platforms to protect customers' private data, which is necessary in the modern era. The utilization of the 3PAKE method has a wide range of advantages. In particular, the 3PAKE protocol offers bilateral verification and secure data transmission. For example, an authorized trustworthy host aids in interactions between buyers and sellers within the e-commerce setting.

In addition to this, the enhanced 3PAKE protocol has some drawbacks which include computational resource complexity due to less memory of the computing machine, and dependent on the trust assumptions. The 3PAKE protocol secrecy mainly depends on multifarious trust assumptions, namely the cryptographic primitive's integrity, and the participating entity's trustworthiness which might always not secure true value in distinct real-world settings. During the implementation of the proposed 3PAKE protocol, there has been observed inconsistency in the initial simulation only due to the distinct script, social network platform, and system, which hindered the interoperability and posed certain challenges while implementing the improved 3PAKE protocol in AVISPA software.

## **6.7. Summary**

In this research, a low-cost model based on multiple 3PAKE protocols has been created for a social network model that combines HF and SE for enhanced 3PAKE protocol and SE along with the ECC. The improvised 3PAKE protocol improves the efficiency while preserving the same level of security as earlier techniques without only depending on any server's passcodes. This enhanced 3PAKE-based social network model is less costly and higher resistant to a variety of assaults, including replay as well as cryptanalysis, and similar kinds of real-time attacks. For model validation and

testing, AVISPA software has been utilized in the development of this improved 3PAKE-based model for validity and confidentiality assessment. A statistical efficacy evaluation is conducted on our improved 3PAKE protocol.

Nevertheless, prior investigators have investigated a variety of methods to resist attacks including man-in-the-middle attacks, replaying attacks, including cryptanalysis attacks across systems. However, due to their flaws, which include significant computational difficulty and resource requirements, extant procedures, and approaches, must pay greater focus to develop new, less time-consuming, and more affordable procedures. To begin with, only a single factor has been employed to verify network users. However, this approach is easily hackable, particularly when it comes to password confidentiality. Individuals frequently connect the same login information on numerous websites namely Email, Facebook, and Instagram. Every user's account may be promptly hacked by an unauthorized user, and even an attacker can utilize well-recognized methods including social engineering, guiding to access various systems' assets and apps instead of an authorized user. Credential verification methods relying on HF and SE must be combined to give the extra confidentiality required today versus various attacks to protect the client's identity from unauthorized attacks.

The proper verification of clients across transmission channels is getting more important to safeguard the crucial content of the clients in interaction due to constant technical developments in the fields of computer networks and IT. Since these allow individuals to develop and manage their own identities without the requirement for additional technology, token protection systems offer simple and practical options for user identification. On another side it is more difficult to recall long random patterns, as a result, people select remember option during login on webpages. Furthermore, the passcodes are chosen from a very narrow set of options, thus making them susceptible to endeavors at password breaking. New techniques may provide the appropriate confidentiality to the secured content in genuine interaction as a method of the authorized host. There is a vital necessity to protect the confidentiality of sensitive datasets. Several researchers have created a variety of strategies in the past to provide secret data privacy when two users wish to interact with one another through an authorized connection. Nevertheless, due to extremely quick advancements in transmission networks and the enormous growth in consumer volume throughout the past couple of years via various available pathways, existing techniques face a variety

of difficulties. Therefore, to overcome the abovementioned threats and restrictions of the previously developed approaches, in this research, a novel 3PAKE-based framework for social network secrecy is constructed which is capable of offering desired confidentiality to the user datasets in real-time communication in a significant manner.

# CHAPTER 7 CONCLUSION AND FUTURE WORK

## 7.1. Conclusion

This chapter provides a summary of the research work done for security verification of the social network model using multiple 3PAKE protocols. Furthermore, this chapter also emphasizes the future research roadmap in this field for resolving other data breach-related issues of modern systems in a significant way.

There is a need to build more practical and secure protocols that are resistant to a variety of assaults such as man-in-the-middle, and cryptographic attacks, to offer users the requisite anonymity when communicating with one another. Making use of credential verification techniques is one of the simple but practical ways when giving sensitive private information within transmission procedures. The 3PAKE technique is one of the pragmatic options to preserve confidentiality of the secret information. Various types of password-based verification procedures have been implemented recently. When several users wish to connect to exchange data with one another via the authorized client in the appropriate way, the 3PAKE protocol offers higher data secrecy. To provide necessary anonymity to the users, several researchers implemented and used a variety of 3PAKE algorithms.

Firstly, in this work, an enhanced 3PAKE protocols-based model has been implemented for social network security verification. This model is based on multiple 3PAKE protocols namely the enhanced 3PAKE protocol that is implemented using the HF and SE, as well as the modified 3PAKE protocol that is implemented using the hybrid approach of the SE and ECC. This approach offers the required secrecy for confidential passcodes, session codes, user login validation, and multiple communication messages. Our enhanced 3PAKE protocol-based social network model demonstrates that this is very effective and offers lower computing stages and lesser computational complexities. There has been utilized the AVISPA software to implement and simulate the proposed 3PAKE protocol for social network security verification. The proposed enhanced 3PAKE protocol offers improved performance

metrics in comparison to state-of-the-art protocols. The proposed 3PAKE protocol computes parse timing of 0.000 seconds, search period 0.120 seconds, depth of 4.0 plies, overall visiting nodes 10, and communication phase 2.0. Enhanced 3PAKE protocols are reliable and give low computational complexity. The enhanced 3PAKE protocol is a suitable option for a variety of purposes, especially in cases when resources are limited and user verification is required. Due to the fast growth of clients over constrained networks, confidential data maintenance is one of the challenging tasks. Multiple users connect using an authenticated server in the communication procedure. There have been certain challenges of information breaches in communication using multiple attacks such as brute-force attacks, cryptanalysis attacks, etc. This requires greater recognition to improve and deploy innovative methods that are competent to provide required confidentiality to the users while interacting with one another.

Secondly, there is developed another modified 3PAKE protocol which is based on SE and ECC. This modified 3PAKE protocol also demonstrates that it is highly reliable and trustworthy in social network security validation. The 3PAKE modified version is robust in the present social network framework security verification. In comparison to numerous assaults like cryptanalysis, and man-in-the-middle attacks, the modified 3PAKE protocol is more resistant and reliable. In comparison to the state-of-the-art 3PAKE protocols, the proposed 3PAKE algorithm has very minimal computational complexity. This modified 3PAKE protocol requires a search time of 0.090 seconds and, a parsing period of 0.000 seconds, while the aggregate interaction stages were recognized as 2.0 in the validation. Moreover, the depth plies were obtained at 3.0. Finally, the measured visiting nodes are observed at 20. The measured performance metrics demonstrate that the proposed 3PAKE protocol is highly secure in social network model settings in the modern world.

## **7.2. Future Scope**

There seem to be significant chances for additional studies on the 3PAKE protocol in the future. However, certain researchers implemented 3PAKE methods for distinct security challenges in social network settings. There remains a huge scope for more research on an advanced version of the 3PAKE approach for social network models. Many researchers have enhanced 3PAKE procedures for a variety of reasons in recent years. Thorough investigations in this field of social networks have a

significant potential for more research. Further, more customized protocols may provide needed privacy while fending against diverse hidden attacks on the network. Various research is conducted in this area recently to safeguard individuals' private data in social networks. However, further research can be done to address current problems related to credentials confidentiality and user verification multiple times, thereby improving the social network model security very effectively



# APPENDIX A

---

## 3PAKE Protocol for the Social Network's Secrecy Verification.

---

### 1.1. Enhanced 3PAKE Protocol Specifications

In the enhanced 3PAKE protocol design that is defined in the HLPSL language, the basic roles are three namely the  $pekc_{C_A}$ ,  $pekc_{C_B}$ ,  $pekc_{S_a}$ , which represent the user  $C_A$ ,  $C_B$ , and the authenticated server  $S_a$ , respectively. Herein we are presenting the one basic role that is  $S_a$  as illustrated in A.1. The authenticated server  $S_a$  stands by to obtain the  $REQ_B$ , and  $REQ_A$  from the user  $C_B$  and then forwards  $C_A K_A$  and  $C_A K_B$  to  $C_A$ . At the similar instance state  $S_t$  of the authenticated server,  $S_a$  will be altered via 0 to 1. There are certain symbols utilized in the basic role of  $S_a$  are described in Tab. 2.

**Table 2:** Illustrates the symbols used in the  $S_a$  role

| S. No. | Symbols            | Meaning of the used symbol           |
|--------|--------------------|--------------------------------------|
| 1      | Hash (.)           | Represents hash function             |
| 2      | Snd (M)            | Forward message                      |
| 3      | $C_A$              | Identity of the first user           |
| 4      | $C_B$              | Identity of the second user          |
| 5      | $S_a$              | Authenticated server                 |
| 6      | $PW_{ax}, PW_{bx}$ | Represents symmetric keys used       |
| 7      | Rcv (M)            | Represents obtained message M        |
| 8      | new ()             | Originate an arbitrary no. used once |

### 1.2. Security Analysis of Enhanced 3PAKE Protocol

Initially, the authenticated server  $S_a$  obtains a message  $(C_B, Gy'.\{C_B, Gy'.Nb'\}_{Hash(C_B, Gy'.PW_{bx})}, C_A, Gx'.\{C_A, Gx'\}_{Hash(C_A, Gx'.PW_{ax})})$  via Rcv () function. After that, authenticated server  $S_a$  selects its own arbitrary number  $N_z'$  as well as evaluates  $Gxz'$ . Lastly, authenticated server  $S_a$  forwards message  $\{Gx'.C_B, Gyz', Nb'\}_{Hash(C_A, Gx'.PW_{ax})}, \{Gy'.C_A, Gxz'\}_{Hash(C_B, Gy'.PW_{bx})}$  via Snd () function. In this article, the authors utilized the DHKE scheme for the designing of the enhanced 3PAKE protocol based on the hash function and symmetric encryption for the social

network's privacy and secrecy. After defining basic roles instantly, there is a requirement to describe the composed roles that further define the new sessions for the enhanced 3PAKE protocol. Fig. A.1 illustrates the role of the authenticated server  $S_a$  for the enhanced 3PAKE protocol for the social network's secrecy verification. Fig.A.2 illustrates the session role for the enhanced 3PAKE protocol for the social network's secrecy verification.

### 1.3. Informal Security Analysis

Within all session's fragments, every basic role namely the  $pek_c_{C_A}$ ,  $pek_c_{C_B}$ , as well as  $pek_c_{S_a}$  have been instanced with solid logic. In the end, a high-level role is an environment at all times described. The environment role comprises universal constants as well as an arrangement of one or more sessions. Fig. A.3 illustrates the environmental role of our enhanced 3PAKE protocol for the social network's secrecy verification. Herein,  $i$  is utilized to represent the intruder that takes part in the implementation of the enhanced 3PAKE protocol utilizing a solid session. It is utilized for the detection of man-in-the-middle assaults. Herein, statement category channel (dy) symbolizes the intruder prototypical namely the Dolev-Yao model. By utilizing this model, the interloper has overall control of the network in such a manner that every message forwarded by the users would pass via the interloper. This interloper can analyze or enhance coming messages as soon as get to know demanded codes. As a result, users can transmit as well as receive data on any route they wish; the intended relationship among specific channel characteristics is preserved.

```

role pek_c_S_a (C_A, C_B, S_a
    : agent
    Snd, Rcv      : channel (dy),
    PW_ax, PW_bx : symmetric_key,
    G             : text,
    Hash         : hash_func)
Played_by S def=
    local S_t     : nat,
    Nz           : text,
    Nb           : text,
    Gx, Gy       : message,
    Gyz, Gxz    : message
    init S_t := 0
    transition
    S_t = 0 /\ Rcv (C_B, Gy', {C_B, Gy', Nb'})
            _Hash (C_B, Gy', PW_bx), C_A, Gx'.
            {C_A, Gx'}_Hash (C_A, Gx', PW_ax)) = |>
    S_t' := 1 /\ Nz' := new()
            /\ Gxz' := exp (Gx', Nz')
            /\ Gy' := exp (Gy', Nz')
            /\ Snd ({Gx', C_B, Gyz', Nb'})
                _Hash (C_A, Gx', PW_ax),
                {Gy', C_A, Gxz'}_Hash (C_B, Gy', PW_bx))
            /\ witness (S_a, C_A, auth_a_s_gx, Gx')
            /\ witness (S_a, C_B, auth_b_s_gy, Gy')
end role

```

**Figure. A.1** Illustrates the role of the authenticated server  $S_a$  for the enhanced 3PAKE protocol for the social network's secrecy verification.

1. Session role for the enhanced 3PAKE protocol (See Figure A.2)

```

role session (CA, CB, Sa
              PWax, PWbx,
              G
              Hash
              : agent
              : symmetric_key,
              : text,
              : hash_func)
def=
  local CA_SND, CA_RCV, CB_SND, Sa_SND, Sa_RCV: channel (dy)
  composition
  pekc_CA(CA, CB, Sa, CA_SND, CA_RCV, PWax, G, Hash)
  /\ pekc_CB(CA, CB, Sa, CB_SND, CB_RCV, PWbx, G, Hash)
  /\ pekc_Sa(CA, CB, Sa, Sa_SND, Sa_RCV, PWax, PWbx, G, Hash)
end role

```

**Figure. A.2** Illustrates the session role for the enhanced 3PAKE protocol for the social network's secrecy verification.

2. The environmental role of the enhanced 3PAKE protocol for the social network's secrecy verification. (See Figure A.3)

```

role environment ()
def=
  const
  a, b, s, i
  PWax, PWbx, PWi
  d
  hash
  auth_a_b_nb
  auth_b_a_dx
  auth_a_s_gx
  auth_b_s_gy
  sec_a_b_gxyz
  intruder_knowledge = {i, a, b, s, pwi, g, hash}
  composition
  session (a, b, s, PWax, PWbx, g, hhash)
  /\ session (a, b, s, PWax, PWbx, g, hhash)
  /\ session (i, b, s, PWi, PWbx, g, hhash)
  /\ session (a, i, s, PWax, PWi, g, hhash)
end role

```

**Figure. A.3** Illustrates the environmental role of the enhanced 3PAKE protocol for social network secrecy verification.

3. Illustrates the analysis goals for the enhanced 3PAKE protocol for the social networks (See Figure A.4)

Fig. A.4 illustrates the analysis goals for the enhanced 3PAKE protocol for social network secrecy verification. We have analyzed the under-mentioned properties that

are considered within the goal section. Herein symbol  $auth_{C_A S_A gx}$  means user  $C_A$  validates  $S_a$  over  $gx$ . Fig. A.4 illustrates the simulation outcomes by OFMC back-end for the enhanced 3PAKE protocol for social network secrecy verification.

```
goal
  authentication on auth_C_A_S_A_gx
  authentication on auth_C_B_S_A_gy
  authentication on auth_C_A_S_B_nb
  authentication on auth_C_B_S_A_gx
  secrecy_of sec_a_b_gxyz
end goal
```

**Figure. A.4** Illustrates the analysis goals for the enhanced 3PAKE protocol for the social network's secrecy verification.

```
SUMMARY
SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/avispa/web-interface-
  computation/./tempdir/workfileEdDMf1/3PAKE.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.12s
  visitedNodes: 10 Nodes
  depth 4 plies
```

**Figure. A.5** Illustrates the simulation outcomes by OFMC back-end for the enhanced 3PAKE protocol for the social network's secrecy verification

## APPENDIX B

### 3PAKE method for secrecy verification of the social network model

```
role alex (CLA, SRA, CLB : agent),
% CH is hash function
CH, Mul: hash_func, Snd, Rcv: channel (dy))
Played_by CLA
Def =
local State : nat,
DCLA, UCLA, IDCLA, IDCLB, CRCLA, CQ, CUS: text,
HCLA, RCLA, RCLB, KCLA, CCLASRA, CSRAKCLA: message,
Inc : hash_func
const alex_server, server_max, alex_max, alex_server,
Subs1, subs2, subs3 : protocol_id
Init State :=0
transition
1. State = 0 ∧ Rcv (start) = |>
State' := 1 ∧ DCLA' := new ()
∧ UCLA' := Mul (DCLA'. CQ)
∧ RACLA' := new ()
∧ HCLA' := CH (RCLA'. DCLA')
∧ RCLA' := Mul (HCLA'. CQ)
∧ KCLA' := Mul (DCLA'. USRA)
∧ CCLASRA' := CH (CIDCLA. CIDCLB. CRA'. KCLA')
∧ Snd (CIDCLA. CIDCLB. CRCLA'. KCLA')
∧ Secret ({CDCLA'}, subs1, {CLA, SRA})
2. State = 1 ∧ Rcv (RCLB. CSRA') = |>
State' := 2 ∧ CK' := Mul (CHCLA. RCLB)
∧ SRAKCLA' := CH (CIDCLA. CIDCLB. RCLA. RCLB.K')
End role
```

**Figure. B.1** Illustrates the specified role for the authenticated client CL<sub>A</sub> in the HLPSL simulator.

```

role max (CLB, SRA, CLA : agent),
% CH is hash function
CH, Mul: hash_func, Snd, Rcv: channel (dy))
Played_by CLB
Def =
local State : nat,
DCLB, UCLB, IDCLB, IDCLB, CRCLB, CQ, CUS: text,
HCLB, RCLB, RCLA, KCLB, CCLBSRB, CSRBKCLB : message,
Inc : hash_func
const alex_server, server_max, alex_max, alex_server,
Subs1, subs2, subs3 : protocol_id
Init State :=0
transition
1. State = 0 ∧ Rcv (start) = |>
State' := 1 ∧ DCLB' := new ()
∧ UCLB' := Mul (DCLB'. CQ)
∧ RACLB' := new ()
∧ HCLB' := CH (RCLB'. DCLB')
∧ RCLB' := Mul (HCLB'. CQ)
∧ KCLB' := Mul (DCLB'. USRB)
∧ CCLBSRB' := CH (CIDCLB. CIDCLA. CRB'. KCLB')
∧ Snd (CIDCLB. CIDCLA. CRCLB'. KCLB')
∧ Secret ({CDCLB'}, subs1, {CLB, SRB})
2. State = 1 ∧ Rcv (RCLA. CSRB') = |>
State' := 2 ∧ CK' := Mul (CHCLB. RCLA)
∧ SRAKCLB' := CH (CIDCLA. CIDCLB. RCLA. RCLB.K')
End role

```

**Figure. B.2** Illustrates the specified role for the authenticated client CL<sub>B</sub> in the HLPSL simulator.

```

role server SRA (SRA, CLA, CLB : agent,
% CH is hash function
CH, Mul: hash_func,
Snd, Rcv: channel (dy))
played_by SRA
Def =
local State : nat,
DSRA, UCLB, UCLA, IDCLA, IDCLB, CRCLB, CQ, CUSRA: text,
HCLB, RCLB, RCLA, SRAKCLB, CCLBSRA, CSRAKCLB : message,
Inc : hash_func
const alex_server, server_max, alex_max, alex_server,
Subs1, subs2, subs3 : protocol_id
Init State :=0
transition
1. State = 0 ∧ Rcv (CIDCLA. CIDCLB. CRCLA'. CKCLA') Rcv (CIDCLA.
CIDCLB. CRCLB'. CK .CLB')
State' := 1 ∧ CUSRA' := Mul (DSRA'. CQ)
∧ CKCLACLA' := Mul (DARA'. UCLA)
∧ CKCLBCLB' := Mul (DARA'. UCLB)
∧ CSRACLA' := CH (CIDCLA. CIDCLB. CRA. CRB'. CKCLACLA')
∧ CSRACLB' := CH (CIDCLB. CIDCLA. CRB. CRA'. CKCLBCLB')
∧ Snd (CRCLB. CRSRACLA')
∧ Snd (CRCLA. CRSRACLB')
∧ Secret ({CDSRA'}, subs3, {SRA})
End role

```

**Figure. B.3** Illustrates the specified role for the authenticated server  $SR_A$  in the HLPSL simulator.

```

role session (CLB, SRA, CLA: agent),
CH, Mul: hash_func),
def =
local CSI, CSJ, CRI, CRJ, CTI, CTJ: channel (dy)
composition
Alex (CLA, SRA, CLB, CH, Mul, CSI, CRI)
Server (CLA, SRA, CLB, CH, Mul, CSJ, CRJ)
max (CLA, SRA, CLB, CH, Mul, CTI, CTJ)
End role

```

**Figure. B.4** Illustrates the specified role for the session in the HLPSL simulator.

```

role environment
def =
const CLA, SRA, CLB: agent,
Ch, mul: hash_func,
cida, cidb, cua, cub, cda, cdb, cra, crb, sds, us, cas, cbs, csa, csb,
kka, kkb, ha, hb, ka, kb, raa, rbb: text,
alex_server, server_max, alex_max, alex_server,
subs1, subs2, subs3 : protocol_id
intruder_knowledge = {a, s, b, h, mul, csa, csb, cas, cbs, ra, rb}
composition
session (a, s, b, h, mul)
 $\wedge$  session (s, a, b, h, mul)
 $\wedge$  session (b, s, a, h, mul)
End role

```

**Figure. B.5:** Illustrates the specified role for the environment in the HLPSL simulator.

```

role goal
secrecy_of subs1
secrecy_of subs2
secrecy_of subs3
authentication_on alex_server_raa
authentication_on max_server_raa
End goal

```

**Figure B.6:** Illustrates the specified role for the goal in the HLPSL simulator.

## Bibliography

- [1] U. Can and B. Alatas, "A new direction in social network analysis: Online social network analysis problems and applications," *Physica A: Statistical Mechanics and its Applications*. 2019.
- [2] J. Kim and M. Hastak, "Social network analysis: Characteristics of online social networks after a disaster," *Int. J. Inf. Manage.*, 2018.
- [3] A. Almaatouq, A. Noriega-Campero, A. Alotaibi, P. M. Krafft, M. Moussaid, and A. Pentland, "Adaptive social networks promote the wisdom of crowds," *Proc. Natl. Acad. Sci. U. S. A.*, 2020.
- [4] B. Kovacs, N. Caplan, S. Grob, and M. King, "Social Networks and Loneliness During the COVID-19 Pandemic," *Socius*, 2021.
- [5] X. Huang, D. Chen, D. Wang, and T. Ren, "Identifying influencers in social networks," *Entropy*, 2020.
- [6] K. Musiał and P. Kazienko, "Social networks on the Internet," *World Wide Web*, 2013.
- [7] E. Muller and R. Peres, "The effect of social networks structure on innovation performance: A review and directions for research," *Int. J. Res. Mark.*, 2019.
- [8] C. Cruz, "Social Networks and the Targeting of Vote Buying," *Comp. Polit. Stud.*, 2019.
- [9] I. Momennejad, "Collective minds: Social network topology shapes collective cognition," *Philosophical Transactions of the Royal Society B: Biological Sciences*. 2022.
- [10] D. Palacios-Marqués, J. F. Gallego-Nicholls, and M. Guijarro-García, "A recipe for success: Crowdsourcing, online social networks, and their impact on organizational performance," *Technol. Forecast. Soc. Change*, 2021.
- [11] B. Guidi, "When Blockchain meets Online Social Networks," *Pervasive and Mobile Computing*. 2020.
- [12] M. Alrubaian, M. Al-Qurishi, A. Alamri, M. Al-Rakhami, M. M. Hassan, and G. Fortino, "Credibility in Online Social Networks: A Survey," *IEEE Access*, 2019.



- [13] I. Kayes and A. Iamnitchi, "Privacy and security in online social networks: A survey," *Online Social Networks and Media*. 2017.
- [14] C. M. K. Cheung, P. Y. Chiu, and M. K. O. Lee, "Online social networks: Why do students use facebook?," *Comput. Human Behav.*, 2011.
- [15] K. Xu, S. Zhang, H. Chen, and H. T. Li, "Measurement and analysis of online social networks," *Jisuanji Xuebao/Chinese J. Comput.*, 2014.
- [16] H. Arshad, E. Omlara, I. O. Abiodun, and A. Aminu, "A semi-automated forensic investigation model for online social networks," *Comput. Secur.*, 2020.
- [17] N. Chetty and S. Alathur, "Hate speech review in the context of online social networks," *Aggression and Violent Behavior*. 2018.
- [18] L. Lőrincz, J. Koltai, A. F. Győr, and K. Takács, "Collapse of an online social network: Burning social capital to create it?," *Soc. Networks*, 2019.
- [19] K. K. Kumar and G. Geethakumari, "Detecting misinformation in online social networks using cognitive psychology," *Human-centric Comput. Inf. Sci.*, 2014.
- [20] A. De Salve, P. Mori, B. Guidi, L. Ricci, and R. Di Pietro, "Predicting Influential Users in Online Social Network Groups," *ACM Trans. Knowl. Discov. Data*, 2021.
- [21] W. Jing and X. Zhang, "Online social networks and corporate investment similarity," *J. Corp. Financ.*, 2021.
- [22] L. N. Zlatolas, T. Welzer, M. Hölbl, M. Heričko, and A. Kamišalić, "A model of perception of privacy, trust, and self- disclosure on Online Social Networks," *Entropy*, 2019.
- [23] A. M. U. D. Khanday, Q. R. Khan, and S. T. Rabani, "Identifying propaganda from online social networks during COVID-19 using machine learning techniques," *Int. J. Inf. Technol.*, 2021.
- [24] D. Savage, X. Zhang, X. Yu, P. Chou, and Q. Wang, "Anomaly detection in online social networks," *Soc. Networks*, 2014.
- [25] S. Zhang, T. Yao, V. K. Arthur Sandor, T. H. Weng, W. Liang, and J. Su, "A novel blockchain-based privacy-preserving framework for online social networks," *Conn. Sci.*, 2021.

- [26] E. J. Yoon, "On the security of Lv et al.'s three-party authenticated key exchange protocol using one-time key," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013.
- [27] Z. Tan, "Privacy-Preserving Two-Factor Key Agreement Protocol Based on Chebyshev Polynomials," *Secur. Commun. Networks*, 2021.
- [28] J. Fan, L. Qiao, Y. Cao, S. Liu, W. Zhang, and L. Tang, "A New Password- And Position-Based Authenticated Key Exchange," *Secur. Commun. Networks*, 2021.
- [29] Y. Yujie, "A Survey on Information Diffusion in Online Social Networks," in *ACM International Conference Proceeding Series*, 2020.
- [30] S. Kumar, M. Saini, M. Goel, and B. S. Panda, "Modeling information diffusion in online social networks using a modified forest-fire model," *J. Intell. Inf. Syst.*, 2021.
- [31] L. Jiang and X. Zhang, "BCOSN: A Blockchain-Based Decentralized Online Social Network," *IEEE Trans. Comput. Soc. Syst.*, 2019.
- [32] M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks: Threats and solutions," *IEEE Commun. Surv. Tutorials*, 2014.
- [33] H. Liang, J. Hu, and S. Wu, "Re-attack on a three-party password-based authenticated key exchange protocol," *Math. Comput. Model.*, 2013.
- [34] "Multi-Modal Biometrics Systems: Concepts, Strengths, Challenges and Solutions," *Int. J. Adv. Trends Comput. Sci. Eng.*, 2021.
- [35] D. Kwon, Y. Park, and Y. Park, "Provably secure three-factor-based mutual authentication scheme with puf for wireless medical sensor networks," *Sensors*, 2021.
- [36] E. Gentina, R. Chen, and Z. Yang, "Development of theory of mind on online social networks: Evidence from Facebook, Twitter, Instagram, and Snapchat," *J. Bus. Res.*, 2021.
- [37] G. Shrivastava, P. Kumar, R. P. Ojha, P. K. Srivastava, S. Mohan, and G. Srivastava, "Defensive modeling of fake news through online social networks,"

*IEEE Trans. Comput. Soc. Syst.*, 2020.

- [38] H. Arshad, A. Jantan, G. K. Hoon, and I. O. Abiodun, “Formal knowledge model for online social network forensics,” *Comput. Secur.*, 2020.
- [39] Y. Wang, J. Wang, H. Wang, R. Zhang, and M. Li, “Users’ mobility enhances information diffusion in online social networks,” *Inf. Sci. (Ny)*., 2021.
- [40] Y. Zhang, X. Ruan, H. Wang, H. Wang, and S. He, “Twitter Trends Manipulation: A First Look Inside the Security of Twitter Trending,” *IEEE Trans. Inf. Forensics Secur.*, 2017.
- [41] S. Horawalavithana, A. Bhattacharjee, R. Liu, N. Choudhury, L. O. Hall, and A. Iamnitchi, “Mentions of security vulnerabilities on Reddit, twitter and GitHub,” in *Proceedings - 2019 IEEE/WIC/ACM International Conference on Web Intelligence, WI 2019*, 2019.
- [42] J. R. Saura, D. Palacios-Marqués, and D. Ribeiro-Soriano, “Using data mining techniques to explore security issues in smart living environments in Twitter,” *Comput. Commun.*, 2021.
- [43] J. Paniagua, P. Korzynski, and A. Mas-Tur, “Crossing borders with social media: Online social networks and FDI,” *Eur. Manag. J.*, 2017.
- [44] G. Liu, Q. Yang, H. Wang, and A. X. Liu, “Trust Assessment in Online Social Networks,” *IEEE Trans. Dependable Secur. Comput.*, 2021.
- [45] N. ELİGÜZEL and L. MANLA ALİ, “Analyzing of Cyber-Security Concepts on Twitter,” *Eur. J. Sci. Technol.*, 2022.
- [46] J. Uyheng, T. Magelinski, R. Villa-Cox, C. Sowa, and K. M. Carley, “Interoperable pipelines for social cyber-security: assessing Twitter information operations during NATO Trident Juncture 2018,” *Comput. Math. Organ. Theory*, 2020.
- [47] R. Gómez Martínez, M. L. Medrano García, and J. A. Gallego Vázquez, “Twitter investment alerts for Ibex35 securities,” *Rev. Perspect. Empres.*, 2017.
- [48] F. Salahdine and N. Kaabouch, “Social engineering attacks: A survey,” *Future Internet*. 2019.
- [49] A. Alturki, N. Alshwihi, and A. Algarni, “Factors influencing players’

- susceptibility to social engineering in social gaming networks,” *IEEE Access*, 2020.
- [50] P. Joshi and C. C. J. Kuo, “Security and privacy in online social networks: A survey,” in *Proceedings - IEEE International Conference on Multimedia and Expo*, 2011.
- [51] M. Maqableh, H. Y. Hmoud, M. Jaradat, and R. Masa’deh, “Integrating an information systems success model with perceived privacy, perceived security, and trust: the moderating role of Facebook addiction,” *Heliyon*, 2021.
- [52] I. S. Hamzah, “Personal security on facebook: Threats and solutions,” *J. Komun. Malaysian J. Commun.*, 2021.
- [53] M. S. Farash and M. A. Attari, “An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps,” *Nonlinear Dyn.*, 2014.
- [54] L. Edelson, T. Lauinger, and D. McCoy, “A security analysis of the facebook ad library,” in *Proceedings - IEEE Symposium on Security and Privacy*, 2020.
- [55] G. Sciarretta, R. Carbone, S. Ranise, and A. Armando, “Anatomy of the Facebook solution for mobile single sign-on: Security assessment and improvements,” *Comput. Secur.*, 2017.
- [56] D. K. Naradin, H. Hairuddin, A. M. Ab Malik, and E. S. Kassim, “Online Purchase Intention: Explorations of the Facebook Users’ Psychological Factors,” *Adv. Bus. Res. Int. J.*, 2020.
- [57] J. Shu, “An efficient three-party password-based key agreement protocol using extended chaotic maps,” *Chinese Phys. B*, 2015.
- [58] F. Avorgbedor and J. Liu, “Enhancing User Privacy Protection by Enforcing Clark-Wilson Security Model on Facebook,” in *IEEE International Conference on Electro Information Technology*, 2020.
- [59] S. Matingwina, “Social Media Communicative Action and the Interplay with National Security: The Case of Facebook and Political Participation in Zimbabwe,” *African Journal. Stud.*, 2018.
- [60] R. M. Alsaifi, “Case study of comparing security features of facebook and

- google plus,” *Int. J. Sci. Technol. Res.*, 2018.
- [61] V. K. Takalkar and P. N. Mahalle, “Confidentiality in online social networks; a trust-based approach,” *J. Cyber Secur. Mobil.*, 2015.
- [62] V. K. Takalkar and P. N. Mahalle, “Data confidentiality in Online Social Networks : A Survey,” *Int. J. Sci. Res.*, 2015.
- [63] V. Dimov and F. Eidelman, “Utilizing social networks, blogging and YouTube in allergy and immunology practices,” *Expert Review of Clinical Immunology*. 2015.
- [64] Y. Guo, H. Wu, and X. Zhang, “Steganographic visual story with mutual-perceived joint attention,” *Eurasip J. Image Video Process.*, 2021.
- [65] T. R. Jildeh, K. R. Okoroha, S. T. Guthrie, and T. W. Parsons, “Social Media Use for Orthopaedic Surgeons,” *JBJS Rev.*, 2019.
- [66] K. A. Fehring, I. De Martino, A. S. McLawhorn, and P. K. Sculco, “Social media: physicians-to-physicians education and communication,” *Current Reviews in Musculoskeletal Medicine*. 2017.
- [67] B. Kubheka, “Ethical and legal perspectives on the medical practitioners use of social media,” *South African Med. J.*, 2017.
- [68] F. G. Reamer, “Social work in a digital age: Ethical and risk management challenges,” *Soc. Work (United States)*, 2013.
- [69] S. S. Bull, L. T. Breslin, E. E. Wright, S. R. Black, D. Levine, and J. S. Santelli, “Case study: An ethics case study of HIV prevention research on facebook: The just/us study,” *Journal of Pediatric Psychology*. 2011.
- [70] A. Ranjbar and M. Maheswaran, “Using community structure to control information sharing in online social networks,” *Comput. Commun.*, 2014.
- [71] O. Shulga, “Confidentiality and scam in the internet,” *Univ. Econ. Bull.*, 2021.
- [72] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, “Online social networks security and privacy: comprehensive review and analysis,” *Complex Intell. Syst.*, vol. 7, no. 5, pp. 2157–2177, 2021.
- [73] A. Afzal, M. Hussain, S. Saleem, M. K. Shahzad, A. T. S. Ho, and K. H. Jung, “Encrypted network traffic analysis of secure instant messaging application: A

- case study of signal messenger app,” *Appl. Sci.*, 2021.
- [74] F. Alshakhs and T. Alanzi, “The evolving role of social media in health-care delivery: Measuring the perception of health-care professionals in Eastern Saudi Arabia,” *J. Multidiscip. Healthc.*, 2018.
- [75] A. Mohammadi and H. Hamidi, “Analysis and evaluation of privacy protection behavior and information disclosure concerns in online social networks,” *Int. J. Eng. Trans. B Appl.*, 2018.
- [76] M. Al Duhayyim, H. M. Alshahrani, F. N. Al-Wesabi, M. Alamgeer, A. M. Hilal, and M. Rizwanullah, “Deep learning empowered cybersecurity spam bot detection for online social networks,” *Comput. Mater. Contin.*, 2022.
- [77] B. Kubheka, “Ethical and legal perspectives on use of social media by health professionals in South Africa,” *South African Med. J.*, 2017.
- [78] F. Beato, S. Meul, and B. Preneel, “Practical identity-based private sharing for online social networks,” *Comput. Commun.*, 2016.
- [79] D. Hemalatha, A. Begum, and S. Alex David, “Privacy study on images uploaded in social networks,” *Int. J. Eng. Technol.*, 2018.
- [80] S. S. Bull, L. T. Breslin, E. E. Wright, S. R. Black, D. Levine, and J. S. Santelli, “Case study: An ethics case study of HIV prevention research on facebook: The just/us study,” in *The Ethical Challenges of Emerging Medical Technologies*, 2020.
- [81] G. Nalinipriya and M. Asswini, “A survey on vulnerable attacks in online social networks,” in *Proceedings 2015 - IEEE International Conference on Innovation, Information in Computing Technologies, ICIICT 2015*, 2016.
- [82] V. Estivill-Castro and D. F. Nettleton, “Privacy tips: Would it be ever possible to empower online social-network users to control the confidentiality of their data?,” in *Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2015*, 2015.
- [83] T. Y. Chang, M. S. Hwang, and W. P. Yang, “A communication-efficient three-party password authenticated key exchange protocol,” *Inf. Sci. (Ny)*, 2011.
- [84] O. Ruan, Q. Wang, and Z. Wang, “Provably leakage-resilient three-party

- password-based authenticated key exchange,” *J. Ambient Intell. Humaniz. Comput.*, 2019.
- [85] C. T. Li, C. L. Chen, C. C. Lee, C. Y. Weng, and C. M. Chen, “A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps,” *Soft Comput.*, 2018.
- [86] M. S. Farash, M. A. Attari, and S. Kumari, “Cryptanalysis and improvement of a three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps,” *Int. J. Commun. Syst.*, 2017.
- [87] Q. H. Zhang, X. X. Hu, W. F. Liu, and J. H. Wei, “Improved Verifier-based Three-party Password-authenticated Key Exchange Protocol,” *Ruan Jian Xue Bao/Journal Softw.*, 2020.
- [88] Q. Xie, B. Hu, and T. Wu, “Improvement of a chaotic maps-based three-party password-authenticated key exchange protocol without using server’s public key and smart card,” *Nonlinear Dyn.*, 2015.
- [89] C. Y. Lin and C. H. Fu, “A lightweight three-party authenticated key exchange protocol with XOR-based operation,” *Chung Cheng Ling Hsueh Pao/Journal Chung Cheng Inst. Technol.*, 2016.
- [90] R. Amin and G. P. Biswas, “Cryptanalysis and Design of a Three-Party Authenticated Key Exchange Protocol Using Smart Card,” *Arab. J. Sci. Eng.*, 2015.
- [91] Q. Shu, S. B. Wang, B. Hu, and L. D. Han, “Verifier-based three-party password-authenticated key exchange protocol from ideal lattices,” *J. Cryptologic Res.*, 2021.
- [92] C. M. Chen, W. Fang, S. Liu, T. Y. Wu, J. S. Pan, and K. H. Wang, “Improvement on a chaotic map-based mutual anonymous authentication protocol,” *J. Inf. Sci. Eng.*, 2018.
- [93] S. A. Lone and A. H. Mir, “A novel OTP based tripartite authentication scheme,” *Int. J. Pervasive Comput. Commun.*, 2021.
- [94] R. Muthumeenakshi, T. R. Reshmi, and K. Murugan, “Extended 3PAKE authentication scheme for value-added services in VANETs,” *Comput. Electr. Eng.*, 2017.

- [95] J. Zhao and D. Gu, “Provably secure three-party password-based authenticated key exchange protocol,” *Inf. Sci. (Ny)*, 2012.
- [96] M. Kim, J. Moon, D. Won, and N. Park, “Revisit of password-authenticated key exchange protocol for healthcare support wireless communication,” *Electronics (Switzerland)*, 2020.
- [97] H. Xiong, Y. Chen, Z. Guan, and Z. Chen, “Finding and fixing vulnerabilities in several three-party password authenticated key exchange protocols without server public keys,” *Inf. Sci. (Ny)*, 2013.
- [98] Z. Tan, “An enhanced three-party authentication key exchange protocol for mobile commerce environments,” *J. Commun.*, 2010.
- [99] A. Yin, Y. Guo, Y. Song, T. Qu, and C. Fang, “Two-round password-based authenticated key exchange from lattices,” *Wirel. Commun. Mob. Comput.*, 2020.
- [100] N. W. Lo and K. H. Yeh, “A practical three-party authenticated key exchange protocol,” *Int. J. Innov. Comput. Inf. Control*, 2010.
- [101] E. Ikhaliya, A. Serrano, D. Bell, and P. Louvieris, “Online social network security awareness: mass interpersonal persuasion using a Facebook app,” *Inf. Technol. People*, 2019.
- [102] G. Rathee, S. Garg, G. Kaddoum, D. N. K. Jayakody, J. Piran, and G. Muhammad, “A Trusted Social Network using Hypothetical Mathematical Model and Decision-based Scheme,” *IEEE Access*, 2020.
- [103] C. Borrego, M. Amadeo, A. Molinaro, and R. H. Jhaveri, “Privacy-Preserving Forwarding Using Homomorphic Encryption for Information-Centric Wireless Ad Hoc Networks,” *IEEE Commun. Lett.*, 2019.
- [104] S. Mostafi, F. Khan, A. Chakrabarty, D. Y. Suh, and M. J. Piran, “An Algorithm for Mapping a Traffic Domain Into a Complex Network: A Social Internet of Things Approach,” *IEEE Access*, vol. 7, pp. 40925–40940, 2019.
- [105] G. Yan, G. Chen, S. Eidenbenz, and N. Li, “Malware propagation in online social networks: Nature, dynamics, and defense implications,” in *Proceedings of the 6th International Symposium on Information, Computer and Communications Security, ASIACCS 2011*, 2011.



- [106] Y. Chen, Y. Mao, S. Leng, Y. Wei, and Y. Chiang, "Malware propagation analysis in message-recallable online social networks," in *International Conference on Communication Technology Proceedings, ICCT*, 2018.
- [107] E. Ikhaliya and J. Arreyambi, "Online social networks: A vehicle for malware propagation," in *European Conference on Information Warfare and Security, ECCWS*, 2014.
- [108] S. K. Sheoran and P. Yadav, "Machine Learning based Optimization Scheme for Detection of Spam and Malware Propagation in Twitter," *Int. J. Adv. Comput. Sci. Appl.*, 2021.
- [109] A. O., T. A. F., A. T. B., and A. B. K., "Modelling Malicious Attack in Social Networks," *Netw. Commun. Technol.*, 2020.
- [110] M. R. Faghani and U. T. Nguyen, "Mobile botnets meet social networks: design and analysis of a new type of botnet," *Int. J. Inf. Secur.*, 2019.
- [111] M. R. Faghani and U. T. Nguyen, "A study of xss worm propagation and detection mechanisms in online social networks," *IEEE Trans. Inf. Forensics Secur.*, 2013.
- [112] N. Venkatachalam and R. Anitha, "A multi-feature approach to detect Stegobot: a covert multimedia social network botnet," *Multimed. Tools Appl.*, 2017.
- [113] H. Zhu, C. Huang, and H. Li, "MPPM: Malware propagation and prevention model in online SNS," in *2014 IEEE International Conference on Communications Workshops, ICC 2014*, 2014.
- [114] K. Pak, S. Pak, C. Ho, M. Pak, and C. Hwang, "Anonymity preserving and round effective three-party authentication key exchange protocol based on chaotic maps," *PLoS One*, 2019.
- [115] Y. Tang, Y. Li, Z. Zhao, J. Zhang, L. Ren, and Y. Li, "Improved Verifier-Based Three-Party Password-Authenticated Key Exchange Protocol from Ideal Lattices," *Secur. Commun. Networks*, vol. 2021, p. 6952869, 2021.
- [116] I. Vazquez Sandoval, A. Atashpendar, G. Lenzini, and P. Y. A. Ryan, "PakeMail: Authentication and Key Management in Decentralized Secure Email and Messaging via PAKE," in *Communications in Computer and Information Science*, 2021.

- [117] C. M. Chen, K. H. Wang, K. H. Yeh, B. Xiang, and T. Y. Wu, “Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications,” *J. Ambient Intell. Humaniz. Comput.*, 2019.

## List of Publication

- [1] **To Analysis Various Security and Trust Computation Techniques for Social Networking Model**, International Conference, on Advanced Research in Computer Science and Information Technology (ICARCSIT), Solapur, India 05 March 2021 pp. 26-37, Volume-9, Issue-4 IJACEN-IRAJ-DOIONLINE-18270.
- [2] **A Secure Three-Party Authenticated Key Exchange Protocol for Social Networks**, Computers, Materials & Continua 2022, Tech Science Press, Volume- 71, Issue-3, pp 6293-6305. doi:10.32604/cmc.2022.024877
- [3] **A Literature Survey on Analysis of Social Network Security System**, THINK INDIA JOURNAL, Pune, India January 2019 pp 2245-2262 Vol- 22, Issue-6 doi: <https://thinkindiaquarterly.org/index.php/think-india/article/view/17165>
- [4] **Security Verification of Social Network Model Using Improved Three-Party Authenticated Key Exchange Protocol**. Symmetry. MDPI 2022; pp 1567 Volume-14, Issue -9. doi:10.3390/sym14081567.