Implementation of Wilson Score on Personal Information Distribution for Privacy-Focused Contact Management

Aqiela Fadia Haya(✉) and Cutifa Safitry

University Bekasi, Bekasi, Indonesia
aqiela.haya@student.president.ac.id

Abstract. This paper proposes an improved contact management system that places its main focus on the privacy of its users by providing a user-controlled privacy management process and implements a user verification method using the Wilson confidence interval. The main the advantage of the proposed method is that users will be able to have full access and control on activities done to their data and be able to control how their data is processed and distributed and avoid identity fraud through the provided verification method. The proposed system is applied within an iOS application developed using Flutter and Firebase. The proposed hypothesis is proven trough a set of testing scenarios demonstrating the verification process and calculation method. The calculation used to obtain the verification scores is the Wilson confidence interval, which according to its supported literature review is used commonly for sorting rankings that use community voting. To validate our findings, a model is used to simulate scenarios of the verification method. This resulted in the revelation that the proposed method is able to accurately represent the levels of integrity of verified users.

Keywords: Privacy · Contact Management · Persona · Verification · Information Distribution

1 Introduction

Human beings, from the beginning of time, have relied on communication to understand each other and survive. Even before they were capable of speaking, humans have found ways to express themselves and connect with each other. Information was delivered using means like cave paintings, rock carvings, and more. Over time, humans developed more and more advanced ways of communicating—they invented languages, started writing letters, and even found ways to be in contact with people from the other side of the earth.

In the modern world, communication is made easier than ever, especially with the development of the internet and the introduction of various ways to communicate through it. Now, people can connect with each other with just a single click. From texts, phone calls, and even video calls, there are numerous methods of communication to choose from. Through these means of communication, information is distributed endlessly

B. B. Wiyono et al. (Eds.): ICEMT 2022, ASSEHR 727, pp. 464–478, 2023.
https://doi.org/10.2991/978-2-494069-95-4_55

everyday at very high speeds. This includes personal information that may not be meant for public consumption, and this spread of personal information has become a large concern today.

For years, privacy has been a never-ending concern not only for technology experts, but also the consumers of technology. Information is spread endlessly every day, with or without the consents of those who own it. There is practically no way to solve the concerns of privacy under the current information distribution scene, as the issue lies within the fundamentals of it. It is not possible for personal information to be kept entirely personal, because it is never solely managed by individual entities in the first place.

As a consumer of communication technologies, user want to be in touch with the people they know through modern communication mediums. However, user might want only those who know me personally to be able to contact me, and not anyone else. This is getting harder and harder as time goes. Personal identifiers are used to get in contact with an entity, but nothing can guarantee that these identifiers will only be available to those with real life connections to the entity.

Some common example of personal identifier in modern communication is e-mails, messenger IDs, and phone numbers. While these identifiers provide a very convenient way of communication and reaching people, they are also very vulnerable to being distributed uncontrollably. Once an outside entity gets a hold of one's contact information, it is never truly their own anymore. Said entity is now free to redistribute that piece of information, risking the privacy of its original owner. The original owner no longer has full control of their own personal information, and this can be dangerous. People have had their contact information distributed without their consent, leading up to many privacy issues and even causing things like financial harm. A lot of people misuse the knowledge of other people's contact information to cause inconveniences or even commit fraud.

The uncontrollable spread of personal contact information have become a cause of universal problems such as phishing. Verizon's 2021 Data Breach Investigations Report (DBIR) states that 94% of malware is delivered through e-mails. Another statistical report by Statista reports that 47.3% of all e-mails sent in 2020 were spam. A survey conducted by First Orion in 2020 shows that between 1,000 mobile phone users in the United States, 21% claim to have gotten 50 or more scam calls per month. In the same infographic report, it is mentioned that phone call scams affected Americans 270% more often compared to the previous year. Similar trends are also observed in countries other than the United States. According to Truecaller's 2020 data report, the number of spam calls they identified in 2020 increased by 25% compared to 2019, with the total number of identified spam calls being 145,5 billion calls.

The goal of this study is to provide a new and safer method of contact and/or identity management. This is done by giving users full access to actions taken by outside entities towards their personal information, and allowing them to interfere with these external actions. Below are the parameters that will be used to evaluate the success of this study: (i) Users are able to store their personal information safely in the application (ii) Users are aware of who has a hold of their personal information (iii) Users are able to remove their personal information from other users' devices (iv) Users are able to manage which information they want to give other users access to, and the information given may differ for each user (v) Users are able to access and store another user's information depending on what the other user allows (vi) Users are able to confirm the credibility of other users through verification scores obtained from a crowd verification process.

2 Methods

This study intends to develop an application called Personafy, a contact management application that implements a new system where users are entirely in charge of their personal information. This will be achieved by keeping anonymity at the root of users' identity and sticking to a strict data ownership policy. Personal information will not be managed by any outside entities or systems—the management will be entirely handled by the users themselves. Personafy will only provide features to help users manage their information as they please. Users will be able to control who has access to their data and be fully aware of all actions taken towards it. They will also be able to access other entities' data depending on the permission given by the owners. Additionally, this study aims to demonstrate a system with a new method of identity management that can be implemented in real life to minimize privacy concerns. Figure 1 shows the four main components which will be implemented in the system.

As privacy is the main focus of this study, it is important to keep things strictly anonymous. To implement this, users are identified using a "core identity" that shall never be accessed by any other entity. The core identity will be in the form of an email address. Instead of directly using the core identity to get in contact with other entities, a newly created, minor identity that can be shared for this purpose is used. In this study, the minor identity used will be referred to as a persona. A persona is not the main identifier of a user, and therefore can be terminated and replaced anytime when needed. For example, if a user feels that their persona is spread too much and may cause them harm, they can choose to terminate it and create a new persona as a replacement. A user may own multiple personas and can choose who can contact which persona. Communications will only be conducted through these personas, and no one can have access to the user's

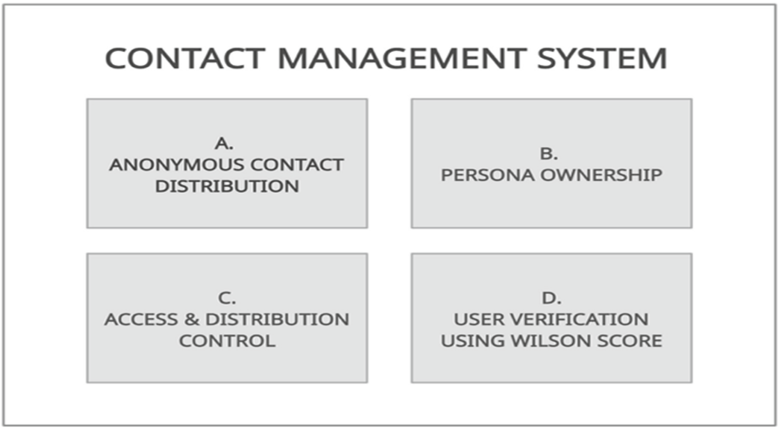

CONTACT MANAGEMENT SYSTEM
A.
ANONYMOUS CONTACT DISTRIBUTION
B.
PERSONA OWNERSHIP
C.
ACCESS & DISTRIBUTION CONTROL
D.
USER VERIFICATION USING WILSON SCORE

Fig. 1. System Components

main identifier. This way, a user's core identity can be kept anonymous at all times and is never at risk of being exploited.

The most important thing in keeping information truly personal and preventing the unwanted spread of it is a clear ownership appointment. Personas should always be associated with its owner and never treated as an independent object. To implement this, personas will be saved in the server along with their ownership details, so the system can always recognize who they belong to. This will ease all processes relating to the protection of privacy.

When an action is taken towards a persona, the system can simply just map out who the persona belongs to and proceed with safety measures from there. If the action is done by an entity that is not the persona owner, the system will immediately notify the owner. The owner is then free to act or not act on this information. As an example, when user A shares a contact information to user B, the owner of the shared contact information is notified about this exchange. If the owner does not agree with the exchange and does not want user B to have access to their contact information, they are able to revoke their contact information from user B's system.

As mentioned previously, all personas are stored in a server instead of locally, and all users will be accessing them from the same source. Access to personas can be revoked anytime by the user owning them. Users can also choose what attributes to show in their personas, which enables them to display different kinds of information to different groups of people.

To implement the idea of giving users full control of their personas and how it's distributed, all actions taken towards the persona need to be documented. These actions include the sharing of a persona done by an outside entity and the storing of a persona in an outside entity's contact list. Since personas are stored in a server and not spread randomly in a disorganized manner, it is much easier for the system to keep track of and document these activities. The system will be able to notify whoever is associated with the persona when an action is taken. These actions will also be available to users—they will be able to access and see all actions related to the personas they own in the form of notifications, making everything completely transparent and minimizing privacy concerns, as users are fully aware of everything happening to their personas.

Figure 2 shows the flow of distribution control in the Personafy application. Users can take extra measures to protect their information and ensure that their information is only distributed with their full consent. If they do not want a certain user to be able to contact them or have access to their persona, then they can simply terminate said user's access to it. This will remove information such as the user's persona and conversations from the other user's system.

One of the biggest threats to privacy and security in the digital world is fraud. When users are able to present themselves freely to others, like how Personafy allows, there is a big risk of identity theft. To prevent this, verification is needed to ensure the validity of each persona and to make sure that users don't fall to the malicious intent of identity thieves.

The Personafy application will implement this by allowing users to verify other users and calculate the Wilson score interval from the statistics obtained. The lower bound of this interval will then be taken and used as the "Verification Score" of each user. The

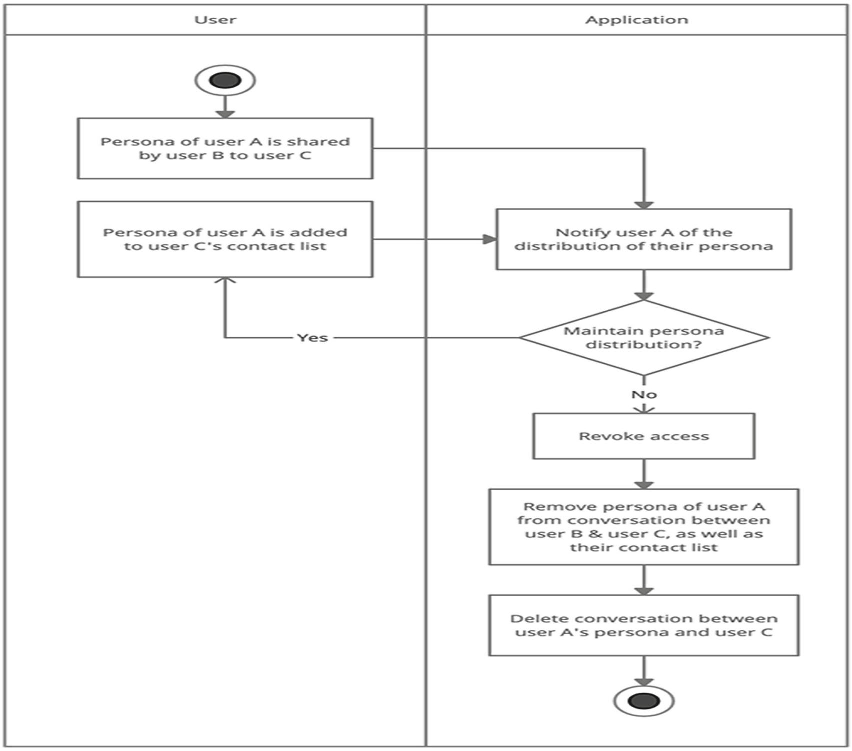

User
Application
Persona of user A is shared by user B to user C
Persona of user A is added to user C's contact list
Notify user A of the distribution of their persona
Maintain persona distribution?
Yes
No
Revoke access
Remove persona of user A from conversation between user B & user C, as well as their contact list
Delete conversation between user A's persona and user C

Fig. 2. Flow of distribution control

Wilson score interval is a confidence interval founded by Edwin B. Wilson in 1927. It is more effective than normal percentages to display ratings, because it also takes into account the total population size to determine the final score.

$$\left(p + \frac{z_{\alpha/2}^2}{2n} - z_{\alpha/2}\sqrt{\left[p(1-p) + \frac{z_{\alpha/2}^2}{4n}\right]/n}\right) / \left(1 + \frac{z_{\alpha/2}^2}{n}\right) \tag{1}$$

Shown above is the equation used to calculate the verification score, or the lower bound of the Wilson confidence interval for a Bernoulli parameter. Parameters of the equation are defined in Table 1.

To obtain the values that will be used in the calculation, the following process in Fig. 3 is conducted. Figure 3 shows the process in which verification is conducted. When a user A has added another user B's persona into their contact list and vice versa, user B will be added into the population count used in the Wilson score calculation and are considered as negative ratings. After reaching a certain amount of interactions, user B will then be prompted to verify the user A. If they choose to verify the user A, then user A's verifier count or number of positive ratings will be increased by 1. If they do not, then the verifier count will stay the same.

Table 1. Parameter Definitions

Parameter	Definition
Positive	Number of positive ratings
Negative	Number of negative ratings
Confidence Level	Confidence level of the ratings
n	Total number of ratings
p	Positive ratings divided by total ratings
zα/2	(1-α/2) quantile of the standard normal distribution, where α = 1 - (Confidence Level)

From here, the verification score will be calculated using the verifier count and population count obtained. The first degree score is calculated using the verifier count and the population count of user A. The second degree score is calculated using the sum of the verifier counts of all users who have verified user A (verifiers), and the sum of the population counts of all verifiers. The results of this calculation will then be displayed for other users to see.

3 Results and Discussion

The contact management system is implemented using Flutter and Firebase, and the developed application is called Personafy. Personafy contains four main pages, which are the Profile, Contact List, Chat, and Notifications pages.

Figure 4 shows the Profile page of Personafy, where the personas of the user are displayed. Users are signed in using their existing Google accounts, and their Google avatar & name are shown on the top of the page. All personas created by the user are displayed in a list, and the Create Persona button is available on top of the list.

Users are able to create as many personas as they want, and all communications with other users will be conducted using these personas. The user's core identity, which in this case is their Google account, will not be exposed to other users under any circumstances. Next to each persona, there are buttons which indicate actions that can be taken by the user towards the personal. The remaining main pages of Personafy are shown in.

Figure 5. The functions of these pages are quite self-explanatory. The two main functions of Personafy are the Revoke and Verification functions. The Revoke function is accessible from three different pages, which are the Profile, Persona Details, and Notification pages.

Figures 6, 7, and 8 show the buttons used to access the Revoke functionality. The Revoke All button on the Profile page removes the persona from the contact list of all users, and the Revoke buttons on the Persona Details page and Notifications page only removes the persona from the corresponding user's contact list. The Revoke button next to a notification about the sharing of a persona removes the message where the persona is shared in the corresponding users' chat room.

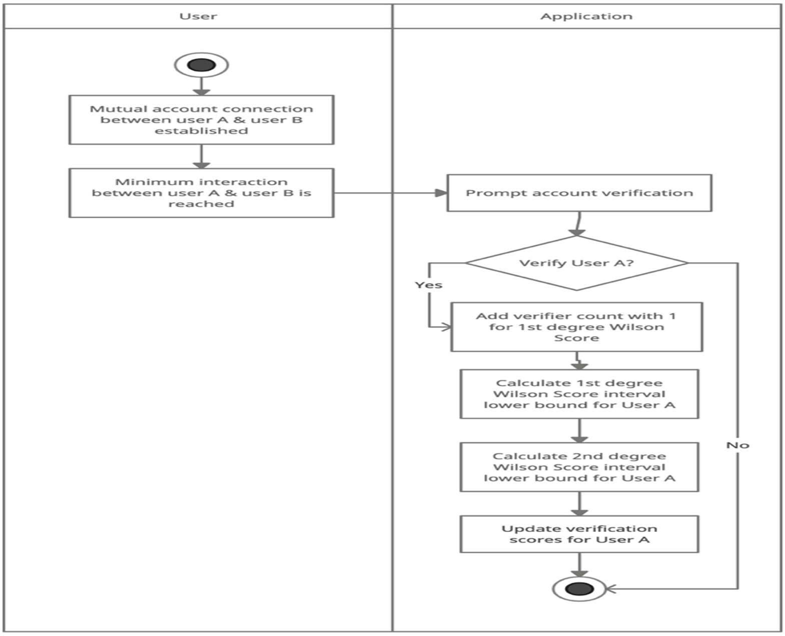

User
Application
Mutual account connection between user A & user B established
Minimum interaction between user A & user B is reached
Prompt account verification
Verify User A?
Yes
No
Add verifier count with 1 for 1st degree Wilson Score
Calculate 1st degree Wilson Score interval lower bound for User A
Calculate 2nd degree Wilson Score interval lower bound for User A
Update verification scores for User A

Fig. 3. Flow of user verification

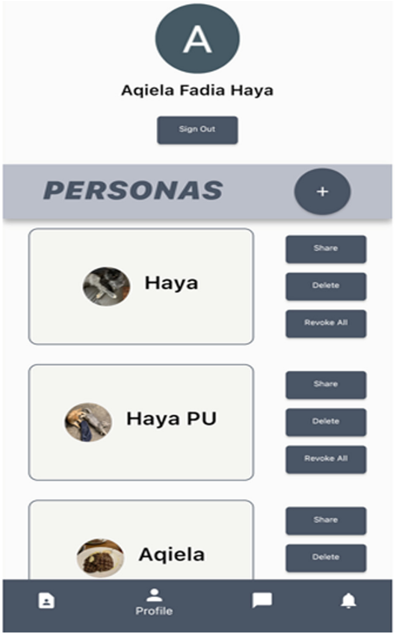
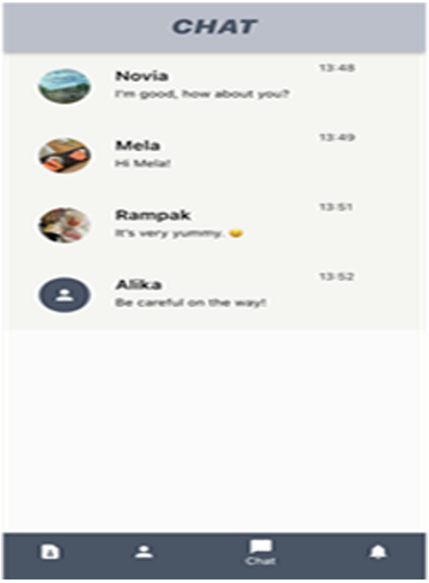


Fig. 4. Profile Page of Personafy



CHAT

Novia 13:48
I'm good, how about you?

Mela 13:49
Hi Mela!

Rampak 13:51
It's very yummy. 😋

Alika 13:52
Be careful on the way!

Fig. 5. Contact, Chat, and Notification pages of Personafy

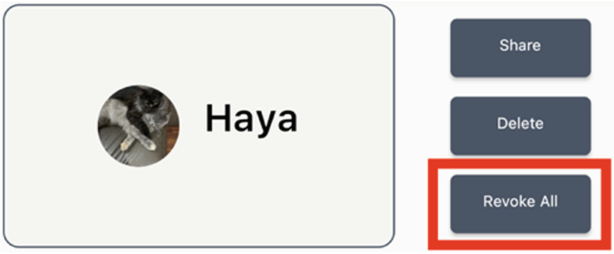
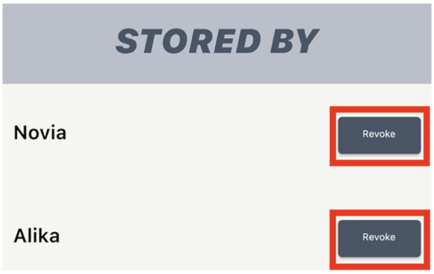


Fig. 6. Revoke All button in Profile page

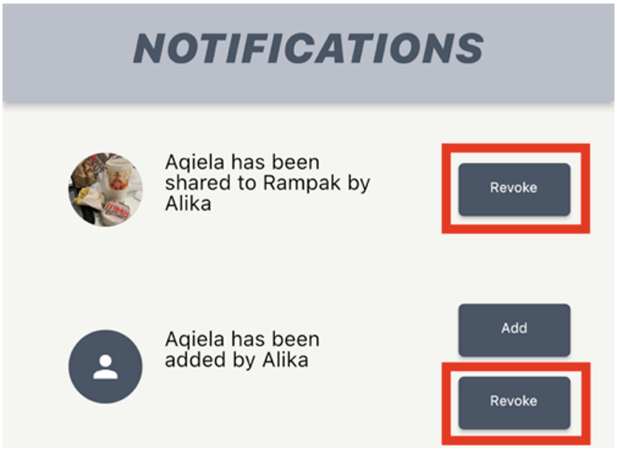


STORED BY

Novia

Alika

Fig. 7. Revoke button in Persona Details page


NOTIFICATIONS

Aqiela has been shared to Rampak by Alika

Aqiela has been added by Alika

Fig. 8. Revoke buttons in Notifications page

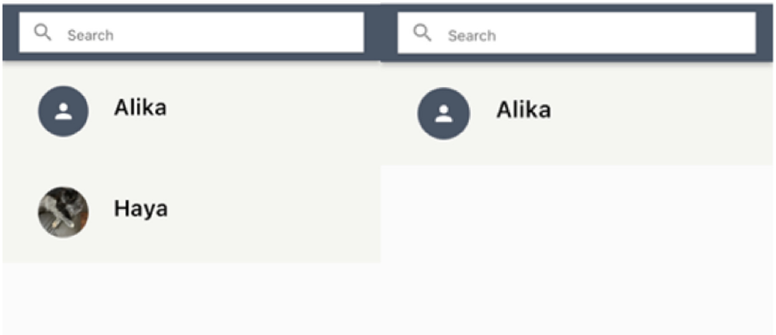
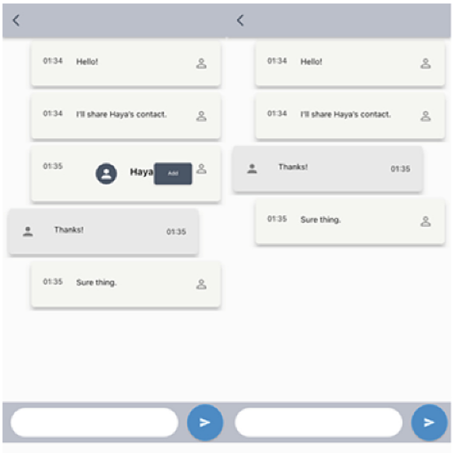


Fig. 9. Contact list of a user before & after a persona is revoked

Figure 9 displays the contact list of a user before and after a persona is revoked. When the owner of the persona decides to revoke the access of the user, the persona is immediately removed from their contact list. Similarly, when a shared persona is revoked from the Notifications page, the persona is removed from the chat room where it was shared, as shown in Fig. 10.

The Verification functionality is prompted when the number of messages within a chat room between two people reach a total of 10 messages. A pop-up asking the user whether they want to verify the contact is shown after they send a message and the number of messages exceed the specified amount, which in this case is 10. Figure 11 shows the verification pop-up when it is displayed in the chat room.

If user clicks Yes, then the verifier count for the contact will be added by 1, and the verification score will be re-calculated. The 2nd degree verification scores of other personas verified by the contact will also be updated accordingly. These scores are available to be checked in the Contact Details page of each contact.



01:34 Hello!

01:34 I'll share Haya's contact.

01:35 Haya

Thanks! 01:35

01:35 Sure thing.

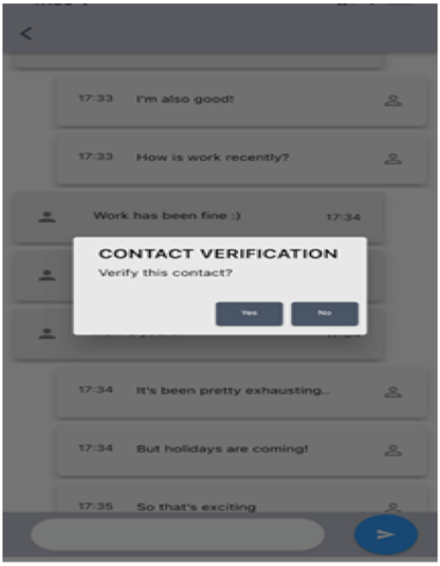
01:34 Hello!

01:34 I'll share Haya's contact.

Thanks! 01:35

01:35 Sure thing.

Fig. 10. Chat room of a user before & after shared persona is revoked



17:33 I'm also good!

17:33 How is work recently?

Work has been fine :) 17:34

CONTACT VERIFICATION

Verify this contact?

17:34 It's been pretty exhausting..

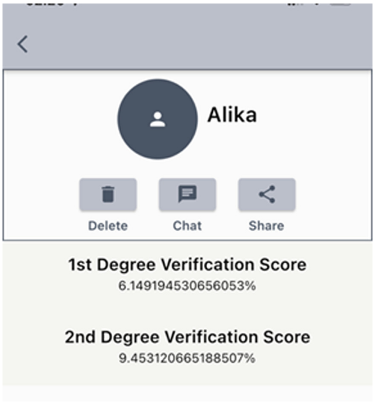
17:34 But holidays are coming!

17:35 So that's exciting

Fig. 11. Contact Verification Pop-up

As shown in Fig. 12, 1st Degree and 2nd Degree Verification Scores are visible to anyone who has the persona added as a contact. From these verification scores, users are able to determine whether they trust the contact and want to continue communications with them.

To demonstrate the verification score calculation for the verification method, two scenarios will be used. The two scenarios will show a difference between the scores in correlation to the sample sizes.



Alika

1st Degree Verification Score
6.149194530656053%

2nd Degree Verification Score
9.453120665188507%

Fig. 12. Verification Scores on Contact Details Page

Table 2. Scenario I Parameters

Parameter	Values for A		Other Values		
	1^{st} Degree	*2^{nd} Degree*	*B*	*C*	*E*
Positive	3	6	2	3	1
Negative	2	3	–	1	2
Confidence Level	0,95				
n	5	9	2	4	3
$z_{\alpha/2}$	1,96				
p	0,6	0,67	1	0,75	0,33

Figure 13 depicts the first scenario, which will be used for verification scenario. In this scenario, a small sample size is used. In the diagram, it can be observed that a user A is verified by three users B, C, and E, and not verified by two users D and F. It is also shown that users B, C, and E, who have verified user A, are verified by 2, 3, and 1 other user(s) respectively. From this diagram, the parameters of the scenario can be mapped out as displayed in Table 2.

Figure 14 represents the second verification scenario. In this scenario, a large sample size is used. Similar to the first scenario, user A is verified by three users B, C, and E. However, users B, C, and E are verified by 30, 45, and 100 users respectively. Below are the parameters used in the calculation as obtained from the diagram (Table 3).

Scenario 1. Figure 6 is a histogram representing the calculation results of Scenario I. In the figure, it is shown that the 1st degree verification score for user A is 23%, and the 2nd degree verification score is 35%. Additionally, the 1st degree verification scores for users B, C, and E are 21%, 30%, and 6% respectively (Fig. 15).

Scenario 2. Figure 7 depicts the calculation results of Scenario II, in which the 1st degree verification score for user A is 23%, while the 2nd degree verification score for

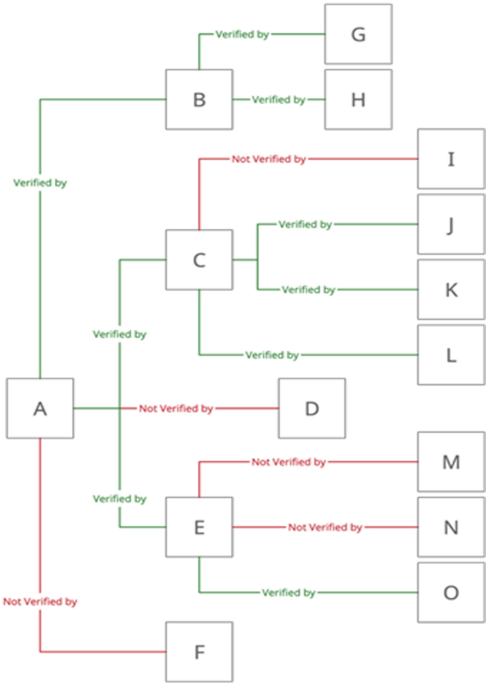


Fig. 13. Diagram of Verification Scenario 1

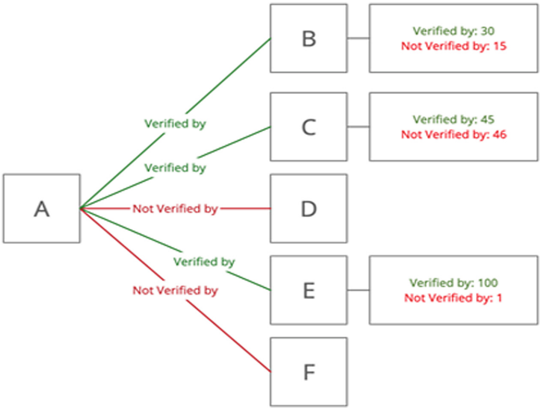


Fig. 14. Diagram of Verification Scenario 2

Table 3. Scenario II Parameters

Parameter	Values for A		Other Values		
	1st Degree	*2nd Degree*	*B*	*C*	*E*
Positive	3	175	30	45	100
Negative	2	62	15	46	1
Confidence Level	0,95				
n	5	237	45	91	101
$z_{\alpha/2}$	1,96				
p	0,6	0,74	0,67	0,49	0,99

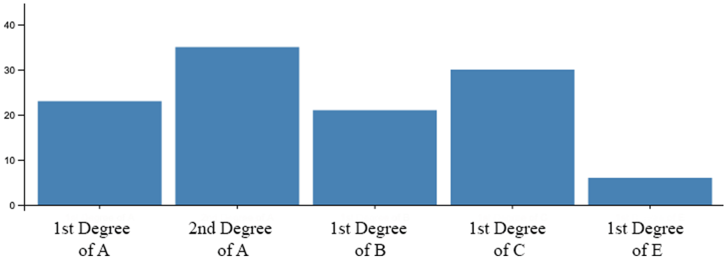


Fig. 15. Result of Scenario I

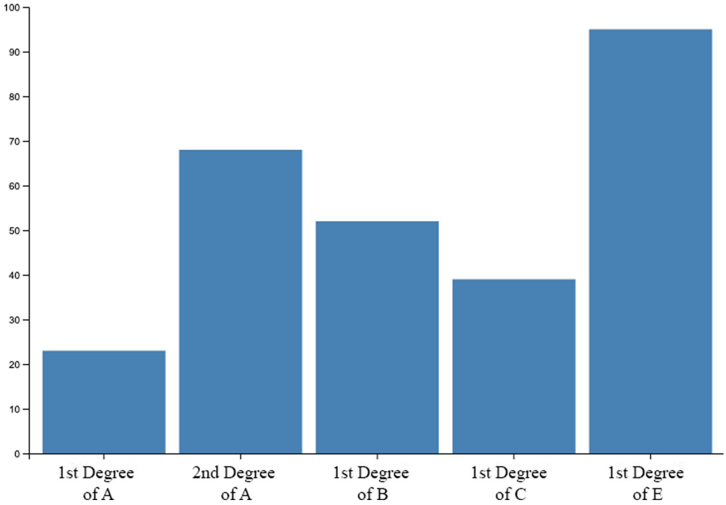


Fig. 16. Result of Scenario II

user A is 68%. The 1st degree verification scores for users B, C, and E are 52%, 39%, and 95% respectively (Fig. 16).

Table 4. Scenario II Parameters

Parameter	A		B	C	E
	1st Degree	*2nd Degree*			
Scenario I	23%	35%	21%	30%	6%
Scenario II	23%	68%	52%	39%	95%

From the calculation results shown above, it can be concluded that the 2nd degree verification score for user A is directly proportional to the 1st degree verification scores of user B, C, and E. This indicates that a user is deemed more trustworthy if their verifiers are also trustworthy.

Comparing the 1st degree scores of users B, C, and E from the two scenarios, it is also observed that the larger the sample size, the higher the verification scores are. This can be seen in the scores of user B in both scenarios. Despite having been verified by 2 out of 2 users in Scenario I, user B earns a higher score in Scenario II where they are verified by 30 out of 45 users, a smaller ratio compared to Scenario I (Table 4).

From the comparison above, it can be seen that Scenario II overall has higher and more reliable scores due to its bigger sample size. As a user, I am more likely to trust another user who is verified by a majority of a larger and trustworthy group of people than a user who is verified by the entirety of a smaller group of people, much like shown in the scores obtained through this evaluation. This proves that the Wilson confidence interval accurately represents the integrity of each user based on the verifications obtained.

4 Conclusion

The Contact Management System proposed in this study consists of four major modules, which are (i) Anonymous Contact Distribution, (ii) Persona Ownership, (iii) Access & Distribution Control, and (iv) User Verification using Wilson Score. From this study, it can be concluded that the personalization of privacy management is beneficial to users, and crowd-based verification methods provide a good alternative to traditional authentication methods. Expansions of this work will further instigate the deployment of this concept and enhance the existing functionalities of the Personafy application. Improvements on the particular module discussed in this paper may also be explored in future researches.

Bibliography

1. Global Identity Foundation. *Identity 3.0 - Principles*, 2018, www.globalidentityfoundation.org/downloads/Identity_30_Principles.pdf. Accessed 23 September 2021.
2. E. Papadopoulou, S. McBurney, N. Taylor and M. H. Williams, "Linking Privacy and User Preferences in the Identity Management for a Pervasive System," 2008 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2008, pp. 192–195, https://doi.org/10.1109/WIIAT.2008.331.

3. Michail Tsikerdekis and Sherali Zeadally. 2014. Online deception in social media. Commun. ACM 57, 9 (September 2014), 72–80. https://doi.org/10.1145/2629612
4. Slomovic, "Privacy Issues in Identity Verification," in IEEE Security & Privacy, vol. 12, no. 3, pp. 71–73, May-June 2014, https://doi.org/10.1109/MSP.2014.52.
5. Jerry O. Talton, Krishna Dusad, Konstantinos Koiliaris, and Ranjitha S. Kumar. 2019. How do People Sort by Ratings? Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, Paper 305, 1–10. https://doi.org/10.1145/3290605.3300535
6. Verizon. *2019 Data Breach Investigations Report*, 2019, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf. Accessed 18 October 2021.
7. Joseph Johnson. *Countries most targeted by malicious mailshots 2020*, 2021, www.statista.com/statistics/420411/spam-malicious-mailshots-target-countries. Accessed 18 October 2021.
8. First Orion. *Infographic: 2020 Scam Call Record*, 2020, https://firstorion.com/infographic-2020-scam-call-report. Accessed 28 September 2021.
9. Truecaller. *Truecaller Insights: Top 20 Countries Affected by Spam Calls in 2020*, 2020, https://truecaller.blog/2020/12/08/truecaller-insights-top-20-countries-affected-by-spam-calls-in-2020-2. Accessed 28 September 2021
10. Edwin B. Wilson (1927) Probable Inference, the Law of Succession, and Statistical Inference, Journal of the American Statistical Association, 22:158, 209–212, https://doi.org/10.1080/01621459.1927.10502953
11. Evan Miller. *How Not To Sort By Average Rating*, 2009, www.evanmiller.org/how-not-to-sort-by-average-rating.html. Accessed 15 October 2021.