© 2017 IJSRSET | Volume 3 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Finding Trustable Software Solutions for Secured Cloud based Services

Varun M Deshpande[1], Dr. Mydhili K. Nair[2]
[1] PhD Student, Department. of C.S.E., Jain University, Bangalore, India
[2] Professor, Department of I.S.E., M S Ramaiah Institute of Technology, Bangalore, India

ABSTRACT
In context of social networking, trust is a very significant requirement and service provider is expected to adhere to highest ethical standards while dealing with user's personal information including personally identifiable information and sensitive information. Service providers face various security challenges such as- web application security threats, privacy breaches and data theft, litigations of intentional or unintentional misuse of user data and business model of social networking requiring social networking services to share user's contextual information with advertisement providers for displaying targeted and contextual advertisements. With all these, they are not well equipped to provide trustable services to users, on their own. Hence, there is need for using external trusted entities to form an interface between service provider and other third parties during data communication involving user's personal information to ensure user privacy is preserved. As user is the primary stake holder in this eco-system., any proposed design should have a user-centric design with which user has a flexibility to choose from different quality of service based service profiles based on their requirements. We present analysis and connect the dots of a string of research contributions for finding rule & policy based trustable software solutions for secured cloud based services.
Keywords: Privacy, Data Security, Digital Identity, Trust

I. INTRODUCTION

A. Value of Trust in Services

One of the primary factors that helps a user to decide on which service provider to choose, is "**Trust**". A belief that one can get a reliable, secure, genuine services and its reputation, contributes to gaining of trust on a given service provider. Unless, a service provider can gain trust of their user base, it can't sustain a business for long. Trust becomes more important topic of discussion when user's assets are at stake. When users trust their assets with the service providers, they expect that, their assets should be kept safe and secure, not misused or leased out to any third party without their explicit consent. We can draw parallel with banking sector. If a bank is found to be fraudulent in handling its user's assets, then quickly users lose trust on the bank and the bank and its leaders are taken to task.

Similarly, in cloud computing and specifically in area of social networking and e-commerce, trust is of paramount importance. The service providers in these sectors deal with personal information of users including personally identifiable information, financial records, contacts, purchase pattern, browsing history etc. which are private. Hence, users have knowingly or unknowingly placed huge amount of trust on service providers such as Google, Facebook, Amazon etc.

With this trust, comes a great responsibility for service provider, of respecting and upholding the trust that users have bestowed on them. The assets that these service providers need to protect are user's personally identifiable information. They need to protect this from malicious agents who can be within the organization such as disgruntled employees or outside the organization such as hackers, third parties like advertisers etc. user's data can be misused intentionally or un intentionally. So, both should be avoided using efficient fool proof mechanisms. The challenges which service providers face to provide trustable software solutions needs to be considered and research community should provide practical and workable solutions to solve these concerns. Varun M Deshpande et. al. [14] highlighted the need to find holistic policy

based approach for working towards trusted computing. Authors underscored the need for external audit system to prove the conformance of policy implementation by service providers.

B. Business Model of Social Networking

Social Networking has taken a firm shape since 2000's with the early success of Orkut, MySpace etc. Later, monopolized by Facebook which serves more than 1.3 billion active users every day and over 2 billon users monthly [10]. The business model that all these social networking sites (SNS) used to attract more people to join them is to provide the service at free of cost. To understand a business model where a commodity or a service is being provided free of cost to billions of users daily, we need to consider their monetization initiatives and financial records. Facebook's 2016 revenue was over $ 27 billion. Which is about $25 per person per year. This conversion rate for a billion user is highly admirable indeed. Varun M Deshpande et. al. [13] discuss in brief about the business model of social networking and why it is important to preserve to avoid context collapse for service providers and advertisers. Along with this, they proposed possible solutions such as secured data sharing policies and identity protection schemes to solve the issue of data privacy with constraint of preserving the business model of social networking.

A deep dive into revenue generating methods from unpaid users direct us to the advertisement and data sharing practices of social networking giants. In a way, commodity that service providers are gaining money is not directly from the social networking web application that they have built. However, it is the users and user generated data that is fueling the financial success and growth of SNS. E-commerce has boomed along with popularity of internet, cloud and social networking. All these sectors are inter linked with each other. SNS are able attract e-commerce service providers like Amazon, Ebay etc. to advertise on their social networking platform as they have an actively engaged audience who are hooked to using their platform.

Greater the number of audience, there is more opportunity for e-commerce web sites who would want to sell their ads on the platform. Along with this, service providers lease out user data to third parties, partners, subsidiaries for financial benefit and to work on certain initiatives to provide better personalized services to the users.

E-commerce websites are investing a lot of money to engage with potential customers through advertising in social networking platforms. To increase the probability of reaching out to perspective customers, they would like to analyze the profile of the user and provide personalized advertisements based on user's personal information such as age, interests, education, occupation etc. and contextual information such as user generated information like status updates, check-in information, activities, content of posts shared, contents of mails and messages received and sent etc. Recently, Facebook announced that it is going to combine the data generated from its subsidiary companies and partners like Whatsapp and Instagram for providing more accurate and contextual user experience. This is one of the reason, when we search for a product on Amazon website and then log into Facebook account, we find several sponsored advertisements from Amazon about similar products on Facebook. We believe that the concept of personalized advertising is at a nascent stage and it is going to evolve to correlate every aspect of our digital life, such as purchase of few products using a credit card, paying bill in a restaurant or watching a movie. All this information leave a digital footprint and this can be aggregated and used to provide targeted advertisements.

C. Quality of Service

Discussion about cloud based applications, is not complete without the topic of "Quality of Service" (QoS). The quantitative and qualitative parameters that define the quality of a service can be used to differentiate one service from another. They can also be used to categorize same service into different quality profiles. Based on the context, the differentiating factors can be decided. In the context of social networking and digital marketing, data security and level of privacy can be suitable candidates for creation of QoS based profiles. In a user-centric design based system, users should be empowered to choose between the available QoS based profiles. A customer, can thus define the service level requirement and agreement between the user and service provider. Varun M Deshpande et. al [5,6] discuss on topics related to QoS based service profiles, and web service ranking and selection based on user requirement. They threw light on customer driven service selection based on their QoS requirements.

D. Web Application Secuirity Challenges

Building a secure cloud based web application has its own challenges which revolve around user data security and privacy. Varun M Deshpande et. al. [9] have discussed about web security challenges which service providers face while building applications. Top ten web security threats published by Open Web Application Security Project's (OWASP) are recognised as a list of standard vulnerabilities which a service provider needs to mitigate during design and development of web services. Following Secure Development Life Cycle (SDLC) and secure coding practices is recommended to avoid the security vulnerabilities from occurring in production environments. Along with this, steps to mitigate major web threats like injection vulnerabilities, Cross Site Scripting (XSS), Cross Site Script Forgery (CSRF) etc. were discussed by the authors. We believe that for building trustable software solutions, building a secure web application which can detect and protect itself from external malicious attack is very important. Unless their data security and privacy is guaranteed by service providers, they can't be trusted with end user's data assets.

It is a known fact that the security falls under the category of nonfunctional requirements. Often, it gets sidelined from more priority requirement of functionality, performance and usability of application. Budget which gets allocated to secure the web application in terms of man power, money and time is limited. Therefore, security needs to be built organically in the system, in each stage of development and release of the product. Optimization of security should act as an enabler of cloud based applications. These aspects related to holistic security program of an organization and proposals for best practices and tools and standards, spanning web application security, privacy and trust management, security operations management and physical security were dealt with by Varun M Deshpande et. al. [1]. They took a case study approach of discussing the current scenario in cloud applications and security. They also explained the requirements of a secure cloud computing along with its objectives and showed to optimize the security of service provider to enable it to perform better within bounds of available resources.

E. Data Privacy Policies and Framework

Users must accept terms of service before signing up with social networking service providers like Google and Facebook. Currently, the data and privacy policies are formed by service providers, themselves. Users must accept the terms of service without which they are not allowed to use the application. Therefore, the rules which are created by the service providers are enforced on end users. They may use the liberty of writing their own privacy policies to take consent from the users for using user's personal data for their financial benefit. One more concern is that privacy laws, which are prevalent in different countries are not the same. While SNS are multinational service providers catering to user base across the globe, they need to abide by rules and regulations which are country and sometimes, state specific. This creates design constraints and lack of uniformity and consistency in laws and legal requirement creates sense of confusion and questions the perception of privacy itself in its true sense.

Users are the reason why the service providers and e-commerce service providers are earning their money. Hence, user's concerns need to be addressed and they should be considered as most valuable stake holders in topic of trustable computing.

These concerns were discussed in depth by Varun M Deshpande et. al. [3,4] by analyzing privacy policies of social networking platforms Google, Facebook and e-commerce websites Flipkart and Amazon.In. They recognized the need for developing solution which does not disrupt the existing business model, yet provide users control over data privacy. In this context, they discussed the need for unified, geo agnostic user centric, holistic, technically correct privacy laws.

II. ANALYSIS OF AVAILABLE SOLUTIONS

A. Introduction

Current work is a connecting the dots of various research works and publications done in "Finding Trustable Software Solutions for Secured Cloud based Services", specifically in social networking and e-commerce. Authors Varun M Deshpande et. al. [1-9, 13, 14] have touched upon various aspects of building a user centric system that addresses security, privacy and data sharing concerns of users, without creating any harm to existing

business model. They also dealt with creation of QoS based service profiles, from which users can choose from based on their requirements.

In this section, we aim to analyze in brief, a list of commercially available solutions for addressing above concerns to user's privacy. An ideal solution is one which addresses concerns of all stake holders without creating a friction between them.

B. Ad-blockers to stop advertisements

One of the existing solutions that was discussed by Varun M Deshpande et. al. [7,8] for addressing online advertisements that are displayed in sponsored sections of websites was the use of ad-blockers. The service providers such as news websites, blogs etc. use sponsored ad spaces to generate revenue. That is how they can sustain and grow their business. When ad-blocker plug-in is used on a browser, it intercepts and blocks the HTTP traffic to and from the sponsored sections on the websites which are meant for advertisements. This blocks all the data sharing to and from the website and advertisement providers as shown in figure 1.

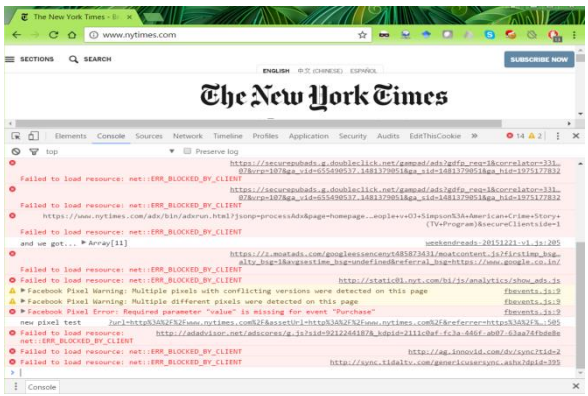


Figure 1. Ad- Blocker plug in used on New York Times

While this temporarily solves concern of data being shared with advertisement providers and advertisement being delivered to the website, it is not a holistic and sustainable solution for below reasons.

- Business model of service provider is affected and they are not able to monetize from the user who accesses their website content.
- Service providers can detect the use of ad-blockers and may block user from accessing website unless the ad-blockers are disabled.
- Even ad-blockers are an online service which requires funds to run. They rely on voluntary donations from their users.
- It creates friction between all stake holders: Users, service providers, advertisement providers and advertisers.

For above reasons, using ad-blockers are not suitable option as this arrangement is not beneficial for any of the stake holders and the business model is not sustainable on the long run.

C. Using Premium Services without Ads

Service providers who provide service free of cost, share the user generated data with third parties to generated revenue. They don't collect money from the users directly. They collect money from their partners and advertisers who sell their ads on service platforms such as SNS.

Alternatively, there is another business model where in service provider provide high quality premium services at a cost to the users. The quality of service is high and they don't sell user generated data to others. This is because they are already collecting money from the end users to safeguard user data.

One of the most relevant examples for these premium service is use of Microsoft Outlook over Google's Gmail service. Organizations who can afford to use Microsoft Outlook, may use this premium product and not worry about their data privacy. However, most of the general users who use Google's Gmail service for personal use are still facing the problem. Other examples are of certain mobile applications which ask users to purchase a paid subscription to stop advertisements. We advise users to read the terms and conditions carefully, especially in these cases; as they may stop sending advertisements to client. However, they may still be sharing user data offline to third parties.

As the data privacy concerns are not addressed for majority of the user base by using premium products, this is not a suitable solution.

D. Not sharing personal information online

Use of social networking and e-commerce websites are a personal choice and no individual is forced into it.

However, collectively as a society, we are moving towards a global village as we build our communication networks. Physical borders are no longer barriers for connecting with people, creating meaningful relationships and to work together on common goals. Hence, we believe that abstinence from social networking or general use of any cloud based web applications that help us connect to anyone in the world is not advisable.

Joe Kissell [11] provides guidelines to his readers to create their own privacy plan while using social networking on any online web portals. In a systematic approach, he provides a list of do's and don'ts while sharing personal information in a social networking platform.

While he does share details on safeguarding one's privacy online, he also alerts the users that the requirement of privacy and business model of SNS don't go hand in hand. The data what has been shared, is virtually an asset of service providers.

If user wants to abstain from social networking or share as less information as possible, it defeats the purpose of social networking and they can't take advantage of the platform. Even the little information that is shared may contain personally identifiable information which is vulnerable to the same web threats which affect other users.

Sharing less information may decrease the level of visibility to others on social networking platform. However, it does not immune the user from the data security and privacy issues which affect every other user on the same platform.

III. PHILOSOPHY OF PROPOSED SOLUTION

A. Introduction

In this section, we aim to throw light on the philosophy and the way of thinking behind various discussions and solutions proposed by Varun M Deshpande et.al. [1-9, 13, 14].

B. User Centric Design Approach

Varun M Deshpande et. al. [2] analyzed various available solutions and then arrived at a suitable and workable solutions that addresses all the concerns related to data security, privacy and data sharing policies of users in social networking and e-commerce and cloud computing in general.

They identified 4 aspects that needed to be dealt with deeply in this context. A suitable solution would come out when all these factors are addressed in the solution. Those 4 aspects are listed below:

- **Trust**
- **Privacy**
- **Data security**
- **Policy driven approach**

They believed that, these 4 factors along with a user **centric design approach** as shown in figure 2, would be ideal for finding trustable software solution for secured cloud based services.

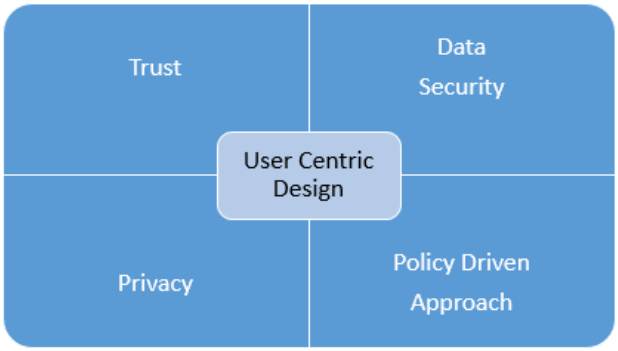


Figure 2. 4 Key Aspects of User Centric Design

We mentioned earlier in the paper, the importance of users in the business model of social networking. The success of SNS is dependent on wide acceptance of the social networking platform by entire online community. Users need to be continuously engaged with the service provider for them to be able to monetize from the users. Users also need to share their personal information such as interests, check-in, likes, dislikes, about their career, education, background etc. All this information about the users are very valuable for service provider. Without these information, they can't build a digital identity of the user and send him targeted and contextual advertisements.

Even for advertisement providers and advertisers, the business will work out if there are huge volumes of engaged users. With the background information on user profile details, specifically targeted advertisements are delivered to users. The sponsored sections in web pages of service providers pull advertisements from backend servers based on user's contextual information.

We can see how important users are for entire eco-system to work. Suppose, one day, if all users stop using social networking sites, then entire business model collapses. Therefore, user, being the most important stake holder in this business eco-system, should get the first preference and the proposed system should always have a user centric design approach. With a user-centric design, the 4 aspects **trust, privacy, data security and policy driven approach** has been incorporated to find trustable solution for secured cloud based applications, specifically targeted towards social networking and e-commerce service providers.

C. Open Standards for Unified Privacy Policy Approach

A successful implementation of any rules and regulations can happen only through policy. Unless the policies are state policies mandated by the governing body, it can't be strictly enforced on the target entities. For example, recently in India, linking Aadhar number (equivalent to Social Security Number) with PAN number (Permanent Account Number) before filing of IT returns (Income Tax returns) for the year 2017 was mandated by government as a policy. As this was a policy mandated by the government, it couldn't be taken lightly by people and they had to abide by the said policy.

In case of data privacy and data security policies, there is no strict unified policy that governs the data usage enforced for service providers. For this reason, they can define their own privacy and data usage policies and enforce it onto the users. There are several short comings with this approach. Varun M Deshpande et. al. [3,4] have brought this out very clearly. Privacy policies of service providers such as Google, Facebook, Flipkart, Amazon.In were analyzed. Few service providers clearly mention that the user's personally identifiable information would be shared with third parties, partners and subsidiaries once user accepts the terms and service of service provider. There are few service providers whose privacy policies says that by mere accessing the website, the user has agreed to service provider's terms and conditions which they have not even seen yet. There are other glaring findings which were discussed in detail by Varun M Deshpande et. al. [4]

Policy requirement differ from one country to other while the service providing entity remains the same. As the data centers are spread across different parts of the globe, user data is distributed and stored in data centers hosted in location different from place of origin. Data privacy laws may vary between place of generation and place of storage which creates controversy regarding jurisdictions of laws and applicable polices. We have seen several legal battles being fought because of this and it is often that service providers are found guilty of violation of laws and are fined a hefty amount.

Above were considered and the authors have recommended that all the stake holders should come together and form a global alliance for creating open standards and unified data privacy policies which are geo agnostic and mandated by all the governments of the world. Stake holders of the eco-system include a global body such as United Nations (UN) to govern and bring together all the nations in a single platform like Paris agreement for fighting against Climate Change. Lawmaking body of each sovereign country. Leading representatives from service providing industry, advertisement providers, e-commerce, researchers, subject matter experts, leaders from security industry etc.

Open standards need to be discussed and agreed upon by all these stake holders. These laws need to reviewed periodically and updated based on requirements. These unified laws need to be mandated for each type of service provider. For example, social networking, e-commerce, health care etc. A set of recommendations and open standards were proposed by Varun M Deshpande et. al. [3] for initial analysis and to deliberate upon.

By enforcing technically correct, and holistic privacy and data security laws, a suitable solution for addressing user privacy issue shall emerge.

D. External Certifying Authority for Real Time Policy Implementation

Transparency is a very important trait of any organization. The most trust worthy organizations are those, which are ready for an external audit always. External audit gives credibility to the claims of the service provider about adherence to certain rules and regulations. Most respected certifying agencies such as ISO (International Standards Organization) etc. give

high level of credibility to the organization under audit. Additionally, a certificate is a proof of merit and validates the authenticity and quality of services provided by the service provider.

When data is being shared between SNS and advertisement provider, personally identifiable information needs to be masked. Unless this happens, user's digital identity is at stake. With service providers like Google and Facebook, they own their own advertisement providing platform. In such cases, data sanitization might not be given as much a priority that it should get as both SNS and advertisement providers belong to same organization. Even otherwise, care must be taken while sharing sensitive data over network as all communication is vulnerable to man in middle attacks and other web application threats.

Suppose, the advertisement providers claim that they are taking care of data anonymization during data sharing, it is not enough. This is because, unless, the process is monitored and continuously audited by external certifying authority, we simply can't trust either the SNS service provider or the advertisement provider. There have been enough instances of data and privacy breaches to argue that data is not safe, unless stringent data security measures are taken and secure data channel is available.

By externally auditing and monitoring the data sharing mechanism continuously in real time, SNS and advertisement providers are given an opportunity to prove their merit and its conformance with proposed open standards and universal data privacy and sharing policies.

The External certifying authority acts as a secure proxy channel for data sharing and it should ensure that data being shared is sanitized. The responsibility of this external agent is more, as it must make sure that, there are no data security loop holes etc.

It is recommended that there be scope for multiple players from security industry for becoming certifying authorities. This is to make sure that there is no monopoly and anti-trust issue resulting from proposed arrangements. The certifying authority may need to publish libraries for secure data channel for integration of code with SNS and advertisement provider.

E. Auditing the Certifying Authority for system transparency

An external certifying authority is entrusted to make sure that unified, geo agnostic, user centric privacy laws are being followed by service provider and advertisement provider. This external certifying authority acts as a trusted third party which is neutral to the system and ensures that privacy policies are being practiced. Also, it ensures that a secure data channel is provided for sanitized data to be shared from SNS to service provider.

We mentioned that authors recommendations are to allow multiple payers from security industry to be external certifying authority. For this to happen, these third-party entities should undergo audit and certification as well from a universally trusted agent. United Nations, under which global alliance for discussion on open standards for data privacy may nominate an empowered body which reports to it. This universally trusted entity is entrusted with certifying these external certifying authorities and to periodically auditing it in a randomized and automated way. This needs to be done so that the external certifying agents are always alert and don't misuse the trust that users have bestowed on them. With this approach, a trustable open standard based data sharing platform can be built.

F. QoS based Service Profiling and Selection

Quality of service plays a crucial role in determining whether we would like to consider using a service from service provider. For example, users would check all the quality of service parameters such as RAM, internal memory, device security mode, camera specifications, screen size, price, battery capacity etc. when we plan to purchase a mobile from an e-commerce web site. Similarly, suppose several service providers are present who are providing same service but with different quality of service parameter. In this case, user should be able to compare the products and based on their requirement, they may choose a service. We can easily understand this with same mobile purchase illustration. Different companies providing similar features. The technical specs can be compared a mobile selected.

Even the same service provider may provide different version of same product which have different quality of service. For example, when we are subscribing to an ISP

provider, at different prices, different download speed and bandwidth is provided.

QoS based profiling is not a new concept for us, as it has been in practice since time immemorial. The choice should be given to the user to compare and chose from the available options. Hence it would lead to customer driven service selection and agreement. With respect to cloud based QoS profiles, customer driven service selection, Varun M Deshpande et al. [5,6] have proposed generic reusable framework on these topics. This can be used on top of the proposed frameworks for choosing between QoS based profiles which have different level of security and privacy.

Specifically, with respect to social networking, QoS based profiling of services by service providers such as Freemium and Premium was recommended by Varun M Deshpande et. al [2,7] where users can choose premium services at their expense and ensure that no user data is shared between SNS and ad- providers. The thinking here is to create an avenue for the end user to take control of what they want themselves. Empowering them to make choices, makes the system transparent and user centric.

IV. PROPOSED SOLUTIONS

A. Introduction

Dealing with user privacy concerns in a holistic perspective, requires thinking of multiple solutions. Each solution is a part of jig-saw puzzle which needs to be assembled in proper way to see the output. In this section, we discuss the proposed solutions by Varun M Deshpande et. al. [2,5,6,7,8] as part of finding trustable software solutions for secured cloud based services. While authors propose solutions for primary objectives in three research papers [2,7,8], secondary requirements of QoS based profiling and service selections have been discussed in two other research papers [5,6].

These solutions have been briefly introduced in the above section. In this section, we discuss more on the contributions discussed in the paper in form of a technical summary.

B. Privacy Preserving Ad-free Social Networking

This paper was the first contribution paper from Varun M Deshpande et. al. [6] The primary objective of the was an idea that, by providing an alternative monetization model for service providers which was more profitable as a substitute to selling advertisements which had privacy concerns.

The proposal was to avoid advertisements in social networking websites by paying a premium amount. They quoted Michel Schreiner et. al. [12] research work, where the authors showed that there is a segment of users who are ready to pay a premium amount for extra privacy preserving capabilities in social networking sites such as Facebook. Primary objectives of this solution document were three-fold.

- Users who don't want their personal information to be shared with advertisement providers and other third parties, should be provided secure opt/out facility as a premium cost.
- This new model should not affect the current business model adversely. If possible, it should create chance for growth.
- The proposed solution should be secure and trustable for all stake holders.

Aligned with the requirements, authors proposed a data sharing model between SNS and advertisement provider which is controlled using a security token. A secure data pipe in which the security token acts as a switch. They proposed a minimum of 2 user profiles, one is common for all unpaid users termed as "Freemium" and other is a paid and privacy protected version termed as "Premium".

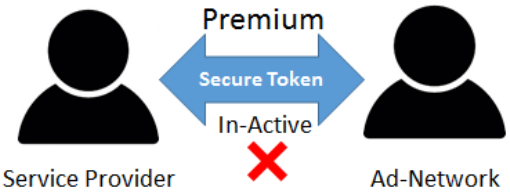


Figure 3. Premium users -Security token inactive

As shown in figure 3, security token that acts as a switch for data communication between SNS and service provider is turned off. So, there is no possibility of user data being shared with third party.

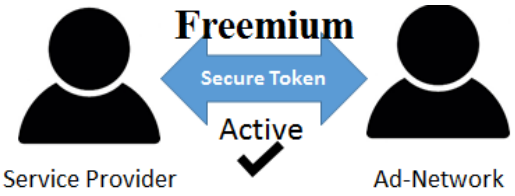


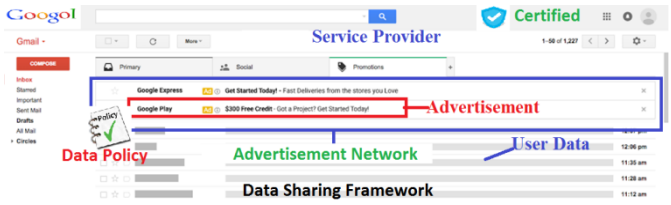
Figure 4. Freemium users – Security Token active

In case of Freemium users, security token is switch on as shown in figure 4. Hence, data sharing channel is turned on. Advertisers can reach their potential customers.

This solution is good because it helps the stake holders of the eco-system in below ways:

- **Premium users**: They can protect their privacy in a secure manner.
- **Freemium users**: Business as usual.
- **SNS**: New mode of revenue generation which is above the average revenue generated per person.
- **Advertisement Providers**: Avoid spending money on users who are not interested in seeing the advertisements.

However, this design doesn't solve the privacy concerns of unpaid "Freemium" users. Hence, further work is required to solve the data privacy issue for all the users even when they are using the service free of cost.



C. Trust based Secure Data Sharing Framework for Social Networking

For the social networking business model to survive, we can't eliminate the e-commerce service providers as they are the entities which are infusing capital into the business model. Without them, the revenue generating options for service providers like Facebook would become very limited and narrow. This would cause a context collapse for the business model and it would subside eventually. Hence, to solve the problem of data privacy, we need to consider that advertisements through e-commerce websites are the primary source of revenue and this channel needs to be protected. However, a holistic solution is one where the scope for making the data communication between SNS and advertisement providers secure, privacy preserving, policy driven and trustable.

Extending the work done with respect to ad-free social networking, authors Varun M Deshpande et. al. [2] proposed a trust based data sharing framework. This framework addresses the privacy issues during data sharing of user's information to and from between SNS and advertisement networks. They retained the idea of multiple QoS based profiles such as "Freemium" and "Premium". Along with this, they added the need for unified privacy policy which is mandated to the service providers. They proposed that open standards for data communications need to setup which would govern the trust based framework.

Additionally, a service provider needs to take get certificate from a trusted third party which acts as a certifying authority and does real time audits for policy implementation. A protective shield should be placed prominently on the website which indicates to users that the privacy is protected on the website by the usage of trust based data sharing framework.

External trusted third party is an auditable component which ensures that the user data communication between SNS and advertisement network is governed by auditable data policies (based on proposed open standards) mandated by law enforcing agencies.

With the proposed trust-based framework, it was clear that we are heading towards a holistic solution for solving user privacy concerns. The main issue which was under consideration was the privacy preservation during data communication. This has been addressed by the trust based framework as shown in above figure 5. On top of proposed framework, holistic and technically sound data privacy policy must be created which ensures that privacy is preserved during data communication.

This proposal in beneficial for all stake holders as below:

- **Premium users:** Can still opt out of advertisements if they desire to
- **Freemium users:** Privacy preserved even if advertisements are shown
- **SNS:** Gains trust from users and community

- **Ad-Networks:** Business as usual with respect to targeted advertisements

D. Identity Protection in Social Networking using Trustable Privacy Preserving Rule based Data Sharing Framework

Trust based data sharing framework discussed in earlier section laid the ground work for identity protection in social networking. This work co-relates all the research work done till date and proposes a trustable privacy preserving rule based privacy preserving rule based data sharing network.

Varun M Deshpande et. al. [8] proposed a model which is an extended version of previous work. In this paper, they propose a framework where the certifying authority is given additional responsibilities of masking sensitive data of the user data context. It is also responsible for creating a secure data channel between SNS, advertisement providers and the backend servers. Name given to this component in current design is "Certified Data Anonymizer"

After analyzing the requirements of advertisement providers, authors realized that genuine ad-networks don't require user's personally identifiable information. They only require as many data points related to the user's interest and their current contextual data. This is to render targeted and contextual advertisements which is beneficial for both ad-network (as there is greater chance for purchase) and user (as the advertisement is relevant to their needs at the time).

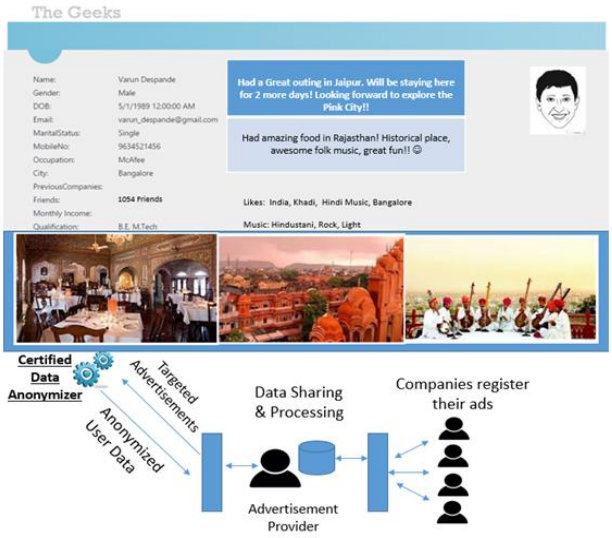


Figure 6. Proposed Framework

Above figure 6, depicts a representation of proposed framework. In the given social networking website, based on user context (status message, check-in etc.), targeted and contextual advertisements are displayed in the sponsored sections of the web page which is reserved for advertisements. The certified data anonymizer converts the user data context which contains personally identifiable information to a sanitized and masked user context. This context contains as many data points which were existing in the original version. However, all the personally identifiable contents would be hidden or generalized based on rules set in the rule engine. For example, instead of giving date of birth, age range is provided. Instead of specific company name in occupation, company category is provided. This is illustrated in figure 7 (original user context) and figure 8 (updated user context)

```
<Data>

<Person>
    <DOB>1989-01-01</DOB>
    <Gender>Male</Gender>
    <Education>B.E,M.S,PhD</Education>
    <Occupation>Mcafee</Occupation>
</Person>

<Books>Chetan Bhagat_Fiction</Books>

<Movies>Hindi|English</Movies>

<TVShows>Animation|Fun</TVShows>

</Data>
```

Figure 7. Original data context

```
<Data>

<Person>
    <Age_Range>25-30</Age_Range>
    <Gender>Male</Gender>
    <Education>B.E,M.S,PhD</Education>
    <Occupation>Corporate</Occupation>
</Person>

<Books>Chetan Bhagat_Fiction</Books>

<Movies>Hindi|English</Movies>

<TVShows>Animation|Fun</TVShows>

</Data>
```

Figure 8. Transformed user data context

This approach is beneficial for both users and advertisement networks as mentioned below:

- **All users:** User privacy is preserved using certified data anonymizer component

- **SNS:** Gains trust and reputation from users and community
- **Advertisement Providers:** Can provide better results as generalized data are search engine friendly.

E. QoS based Profiling and user driven service selection

In this extended segment of research work, authors Varun M Deshpande et. al. [5,6] worked specifically on QoS based profiles on the cloud. QoS parameters can be set with respect to context and based on the service. We explained earlier using example of purchasing mobile and choosing from various ISP profiles. Parameters in these cases are different.

When we draw parallel to QoS profiles in the research papers [2,7] which are based on privacy and data security requirements of user. We believe that users should be given right and flexibility to choose from these QoS based profiles, *dynamically*. Authors have discussed in detail in the research paper [5] business logic for maintaining cloud environment in different QoS profiles and mathematical model and business logic for context switching is provided. Implementing such as system, would enable to provide ability for service provider to securely switch users who are in one QoS profile to another on need basis without any technical glitch.

Users should be provided a mechanism where they can compare between same service offered by different vendors and different QoS profiled services provided by the same vendor. Varun M Deshpande et. al. [6] proposed a generic ranking algorithm which give a relevance score for each contending service based on user preferences and corresponding advertisement done by service provider. The web services are rated on a scale of 0-100% based on level of match between user requirements and advertised QoS of service.

With this approach, user has greater control in choosing the service provider and service profiles based on his requirements. User centric design was a core requirement in our research work. Keeping user's requirements in mind, smart user profiles can be built to attract the users. Newer revenue generating models can be created in the process.

This user-centric approach is beneficial for all for below reasons:

- **All users**: Can take an informed decision on which service/profile to be used for his custom requirements.
- **SNS**: Gains trust, popularity and reputation from users. Newer revenue generation methods can be formed thus.
- **Advertisement Providers**: Can target specific users for specific advertisements based on their QoS profile preference.

This research based proposals complete a holistic user centric design framework for finding trustable software solutions for secured cloud based services.

V. ANALYSIS OF RESULTS

A. Introduction

In previous sections, we have discussed the proposed solutions and understood the methodology used and resultant user-centric design. In this section, we analyze key aspects which need to be read between the lines.

B. Why we can't trust service providers with user's personal information

We have discussed the importance of gaining user's trust to be successful in the running the business in service industry. Trust means that one party is entrusting some of their valuable assets with the second party in good will. In case of cloud computing and specifically social networking, user is trusting their personal information with service providers. Service providers need to ensure that data is not leaked out, misused or compromised. However, there are so many web application threats, privacy breaches, intentional and unintentional data access and requirement of data sharing for delivering contextual advertisements etc. which service provider must deal with. Privacy litigations and several anti-trust law suits against major service providers make it hard for us to single handedly trust all of user data with SNS. *Even their data policies suggest that once they share information with third parties, they are not responsible on how the third parties use the information.* Considering all this, we can't trust service providers with user's personal information. Especially so with respect to data sharing policies.

C. Need for Transparent Trustable Solutions

Trustable solution in our context implies that some external trusted entity is guaranteeing the user about for data privacy and security. The trusted third party takes the responsibility of certifying and auditing the data communication between SNS and advertisement providers, it gives confidence to the users that their data is secure and they can go about their business with peace of mind. All the facilities provided by social networking can be used with knowledge that their personal information will not be misused during targeted with contextual advertisements. Certifying authorities take care of real time policy implementation and auditing. They are also responsible for a secure communication channel for data sharing.

D. Similar Solutions implemented in other Knowledge areas

For secure communication between any two entities, there needs to be a neutral third party who will stand by as a trusted evidence and a symbol of integrity for both parties. The validation of certifying authority is final and binding which both parties need to agree. Like solutions described in this paper, there have been several examples where a certifying authority is used as a neutral and trusted entity for secure transactions. Some of them are listed here:

- **Use of Trusted Certifying Agents in Transport Layer Encryption using HTTPS :** Several certifying agents like Comodo, Verisign etc. provide certificates to web applications which certify that all the client to server communication that happen in the website are encrpyted and hence safe. In this case trusted entities are Comodo, Verisign etc.
- **Use of Trustable agent for authentication in secure Banking Transaction :** RSA encryption based secureity tokens are used during banking transaction to ensure that bank securely authenticates the user beyond just logging into the banking portal. In this case, RSA security token providers are trusted agents which validated the authenticity of transaction.
- **Using Trusted Certifying Authority in generating Digital Certificates:** There are digital certificate issuing authorites which take care of validating documents with digtal signatures which is a proof that document was accessed and authorised by the people who generate the digital certificate. In this case digital certificate issuing authorities act as trusted entities.

Hence, use of trusted third party entities is not a new proposal. However, using the concept for purpose of data privacy and the way certifying authority is being used as a certified data anonymizer and secure channel for data communication is unique to the solutions discussed in the paper.

VI. CONCLUSION AND FUTURE SCOPE

We began the paper by discussing value of trust in service industry and how it can make or break a business. We then understood the business model of social networking and how data sharing is an inseparable component in it. Web application security challenges for data security and privacy which every cloud based application faces were put forth.

As the title suggests, the authors have tried to understand the requirements of secure cloud based services. Available solutions for solving user's data privacy issue were analyzed; such as use of employing of ad-blockers which are freely available, use of premium services by paying the cost for it etc. We proved that these options don't provide holistic solutions for users.

Current work is a concluding remark on list of contributions done by Varun M Deshpande et. al [1-9, 13, 14] for achieving our research goals. The paper does the job of connecting the dots to prepare complete picture of the solution. They started by reviewing all the existing security challenges, requirements, web application threats etc. and proposed that optimization of security is required to enabled cloud applications.

Then, authors analyzed privacy policies from top service providers and brought forward the short comings on current way of handling privacy and data security policies. We proposed that there is a need for developing open standards for data privacy policies and these policies need to be unified, universal, geo agnostic and mandated from all the lawmaking bodies of each country. We have proposed initial set of standards as well.

We specifically considered problem of untrustworthy data sharing practices between SNS and advertisement

providers. For providing a trustable and privacy preserving solution, we must intercept this data communication, introduce a trusted third party as a certifying authority and certified data anonymizer. We also proposed QoS based profiles and introduced security tokens which can be used for secure ad-free social networking. With all these contributions, we could build trustable data sharing framework for privacy preserving social networking.

We discussed creating user centric design using QoS based cloud profiling and dynamic context switching which enable to change their QoS profile based on their requirement on the go. This secure user-centric model is built on top of privacy preserving social networking using trustable rule based anonymization.

Overall, we discussed the philosophy and thought process behind finding solutions for the given research problem. We then gave a technical summary of all the research contributions made towards the topic. We highlighted the implications for all the stake holders as well.

As security researchers, we have a great opportunity to solve real world unsolved problems. Digital privacy and data security in social networking are hot topics which require urgent attention in security research. We took on the challenge of finding trustable software solution with a user centric design for this problem and arrived at above discussed solutions. We now have the responsibility of taking these results to real world implementations.

The consolidated research work has room for further progress and opportunities for improvement. Sophisticated rule engines for data anonymizations could be built. This was not considered during current research work. Open consortium needs to be formed for discussions related to unified data privacy policies and create awareness for the same. Solutions discussed in the contributions are applicable for real time data communications only. This solution can be extended to off line aggregate data communication between SNS and third parties.

VII. REFERENCES

[1]. Varun M Deshpande, Dr. Mydhili K. Nair, Ayush Bihani, "Optimization of Security as an Enabler for Cloud Services and Applications", book chapter to be published by Springer in edited volume titled "Cloud Computing for Optimization: Foundations, Applications, Challenges", to be published in "Studies in Big Data" book series, Springer (2017)

[2]. Varun M Deshpande, Dr Mydhili K. Nair, "Trust based Novel Secure Data Sharing Policy Framework for Social Networking", published in International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), Vol4, Issue 6, June 2017, Online ISSN- 2394-2320, with Impact Factor 4.890

[3]. Varun M Deshpande, Dr Mydhili K. Nair, "Open Standards for Data Privacy Policy Framework in context of Trusted Social Networking", to be published in International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) | Volume 2 | Issue 5 | August - 2017 ISSN: 2456-3307

[4]. Varun M Deshpande, Dr Mydhili K. Nair, "Need for User Centric & Unified Privacy and Data Policies for Social Networking. Case Study: Google, Facebook, Amazon & Flipkart", to be published in International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137, Volume – 02, Issue – 08, August – 2017, PP – 83-93

[5]. Varun M Deshpande, Dr. Mydhili K. Nair, Balaji Sowndararajan(2013), "Customer Driven SLA in Cloud Based Systems", published in Proceedings by Elsevier of International Conference of Emerging Computations and Information Technologies, SIT, Tumkur, Karnataka (India), 22-23 November, 2013, pp 508-518

[6]. Varun M Deshpande, Dr. Mydhili K. Nair (2014), "Anveshana – Search for the Right Service", published in Proceedings by IEEE of International Conference of Convergence of Technology, Pune, Maharastra (India), ISBN 978-1-4799-3759-2

[7]. Varun M Deshpande, Dr. Mydhili K. Nair (2017), "A Novel Framework for Privacy Preserving Ad-Free Social Networking", published in Proceedings by IEEE of 2017 2nd International Conference for Convergence in Technology

(I2CT), Pune, Maharastra (India), ISBN 978-1-5090-4307-1/17

[8]. Varun M Deshpande, Dr. Mydhili K. Nair, "Identity Protection in Social Networking using Trustable Privacy Preserving Rule Based Data Sharing Framework", under review in IEEE Transactions on Computers journal, ISSN: 0018-9340

[9]. Varun M Deshpande, Dr. Mydhili K. Nair and Dhrumil Shah, "Major Web Application Threats for Data Privacy & Security – Detection, Analysis and Mitigation Strategies", under review in International Journal of Scientific Research in Science and Technology PRINT ISSN : 2395-6011, Volume 3 | Issue 7 | September-October 2017

[10]. Facebook's Q2 2017 Financial Results, https://s21.q4cdn.com/399680738/files/doc_news/2017/FBQ2'17-Earnings-Release.pdf (Last viewed on 23rd Aug, 2017)

[11]. Joe Kissell, "Take Control of Your Online Privacy", 3rd Edition (Published by TidBITS Publishing, Inc. in April 2017, ISBN: 9781615424856)

[12]. Michel Schreiner, Thomas Hess,2015 "WHY ARE CONSUMERS WILLING TO PAY FOR PRIVACY?AN APPLICATION OF THE PRIVACY-FREEMIUM MODEL TO MEDIA COMPANIES" published in Twenty-Third European Conference on Information Systems (ECIS), Münster, Germany, 2015

[13]. Varun M Deshpande, Dr. Mydhili K. Nair, "Digital Privacy and Data Security in Cloud based services - A Call for Action" under review in Second International Conference on Integrated Intelligent Computing ICIIC-2018) to be published by Springer in Advances in Intelligent Systems and Computing, indexed by Scopus and DBLP

[14]. Varun M Deshpande, Dr. Mydhili K. Nair, "Towards Trusted Social Networking-Need for Holistic Policy based approach", to be submitted in Second International Conference on Integrated Intelligent Computing ICIIC-2018) to be published by Springer in Advances in Intelligent Systems and Computing, indexed by Scopus and DBLP