ISSN: 2306-2495 | RNPS: 2343 *Serie Científica de la Universidad de las Ciencias Informáticas*
http://publicaciones.uci.cu Vol. 14, No. 3 Mes: Marzo, 2021, Pág. 1-30

Tipo de artículo: Artículo original

OSNSDP: A Systematic Approach towards Requirement Capture to Use the Blockchain Technology

OSNSDP: un enfoque sistemático hacia la captura de requisitos mediante la tecnología Blockchain

Idepefo, F.O [1*]
Akhigbe, B.I [2]
Afolabi, B.S [3]

[1] Department of Computer Science and Engineering, Obafemi Awolowo University, Ile - Ife, Nigeria. E-Mail: felixidepefo@gmail.com
[2] Department of Computer Science and Engineering, Obafemi Awolowo University, Ile - Ife, Nigeria. E-Mail: benplus1@gmail.com
[3] Department of Computer Science and Engineering, Obafemi Awolowo University, Ile - Ife, Nigeria.

*** Corresponding author: felixidepefo@gmail.com**

Abstract
The global computing scale of the Internet has made it possible for users globally to Ubiquitously Interact Socially (UIS). This level of interaction and its gains have influenced the cases of privacy disclosures and data breaches, which are rampant due to the vulnerability of users' personal information. The centralized architecture that drives UIS also contributed to this influence. There are also documented evidences of efforts to deal with this and enforce Sensitive Data Protection (SDP). Of particular interest in this paper is the use of the Theoretic of Leveraging the Technology of Blockchain (ToLToB) due to the synergistic techniques it offers to realise SDP. However, the right requirements and methods of elicitation must be applied to use the ToLToB in order to provide deployable software artifacts for SDP among untrusted peers. Interestingly, there is yet no known systematic approach to the best of the authors' knowledge to elicit suitable requirements to use the ToLToB within the context of softwarization for SDP. To fill this gap, this work presents a user requirement engineering-based framework that is reproducible going by the outcomes from its use. These outcomes and paper's contribution include a taxonomy, scenarios, functional and non-functional requirements, and examples profiling of attackers. In the future, personas will be extensively considered along with analysis using theoretic models to further expand and deepen the knowledge and understanding of specific protection mechanisms for online sensitive data.

Keywords: *Internet & information technology; Functional Requirements; Blockchain technology; Sensitive data protection; Requirement engineering.*

Resumen

El desarrollo informático global y el uso de Internet han hecho posible que los usuarios de todo el mundo interactúen socialmente de forma ubicua (UIS). Este nivel de interacción y sus beneficios han influido en la divulgación de privacidad y violaciones de datos, debido a vulnerabilidad, obteniéndose informaciones personales de los usuarios. La arquitectura centralizada que impulsa a UIS también contribuyó a esta influencia. También hay evidencias documentadas de esfuerzos para mitigar y hacer cumplir la Protección de Datos Sensibles (SDP). De particular interés en este artículo es el uso de la Teoría del Aprovechamiento de la Tecnología de Blockchain (ToLToB) debido a las técnicas sinérgicas que ofrece para realizar SDP. Sin embargo, se deben aplicar los requisitos y métodos de obtención correctos para usar ToLToB a fin de proporcionar artefactos de software implementados para SDP entre pares que no son de confianza. Curiosamente, todavía no existe un enfoque sistemático conocido en el mejor de los conocimientos de los autores para obtener los requisitos adecuados para utilizar ToLToB en el contexto del desarrollo de

software para SDP. Para llenar este vacío, este trabajo presenta un marco basado en ingeniería de requisitos de usuario que es reproducible según los resultados de su uso. Estos resultados y la contribución del documento incluyen una taxonomía, escenarios, requisitos funcionales y no funcionales y ejemplos de perfiles de atacantes. En el futuro, las personas se considerarán ampliamente junto con el análisis utilizando modelos teóricos para ampliar y profundizar aún más el conocimiento y la comprensión de los mecanismos de protección específicos para datos sensibles en línea.

Palabras clave: Internet y tecnología de la información; Requerimientos funcionales; Tecnología Blockchain; Protección de datos sensibles; Ingeniería de requisitos.

Recibido: 10/01/2021
Aceptado: 20/02/2021

Introduction

In this age of the Internet, which is a network of Global Computing Scale (GCS), ubiquitous interactive communication with multimodal capacity that transcends space and time has become possible. The GCS offers the capability to socially network among users of all ages globally. This has in turn influenced the current level of Internet penetration with the use of Online Social Networking (OSN) platforms like Facebook, Twitter, LinkedIn, Instagram, etc. that are now part of our daily lives (Graffi, and Masinde, 2020). It is now inevitable for humans in their millions to interact digitally (Graffi, and Masinde, 2020). This has resulted in the generation of huge volume of digital traces (i.e. sensitive users' data) (Iannelli *et al.* 2020). These data require protection since they contain users' personal information. It has become significant to address Online Social Network Sensitive Data Protection (OSNSDP) going by the number of social media users, which today stands at about 3 billion worldwide (Guidi, 2020). The scale of OSN is huge and continues to grow in the number of users and the amount of data uploaded and shared on daily basis (Such and Rivatsos, 2016). For example, a fully filled-out Facebook profile contains about 40 pieces of recognizably personal information. This favours the fact that Facebook has an all-inclusive snapshot of users' personal information and those they know immediately their profile is created (Rathore and Tripathy, 2019).

The literature is replete with reported cases of privacy disclosures and data breaches. This is because users' personal information is vulnerable due to the Centralized nature of the architecture that drives OSN implementation. This makes its mechanism for privacy protection non-resilient to protect users' sensitive data (Fogues *et al.,* 2017). This central authority (Guidi, 2020) gives service providers (e.g., Facebook, Twitter, etc.) control over users' personal information (Bahri *et al.,* 2018) and online censoring of social media platforms without the consent of users (De Salve *et al.,* 2018). Several approaches to decentralize this architecture have been reported in the literature. Cutillo *et al.* (2009) apply the model of privacy preservation in OSN, while a de-anonymization attack model has been proposed by Wondracek *et al.* (2010). In Tai *et al.* (2011) a scheme that re-identifies victims using adversary's information was

developed, while a-victim-prediction-scheme with improved detection accuracy was presented in Zhou and Chen (2020). Similarly, a scheme that allows the partial encryption of OSN was successfully deployed in Schillinger and Schindelhauer (2020) to decentralize OSNs. The sole aim of these contributions were to avoid data breaches from malicious attacks and ensure the control of users' data was not entirely in the hands of social media platform owners. What is of particular interest in this paper is the use of the Theoretic of Leveraging the Technology of Blockchain (ToLToB), which includes a synergy of cryptographic techniques and appropriate consensus mechanism to realise Sensitive Data Protection (SDP).

OSNSDP is possible with the use of the ToLToB to provide deployable software artifacts as solution to manage users' sensitive data among untrusted peers (Casino *et al.,* 2018; Zheng *et al.,* 2018; Ghosh *et al.,* 2020; Guidi, 2020). However, the success of software artifacts that are deployable rely on the use of appropriate functional and non-functional requirements. Interestingly, there is yet no known systematic approach to the best of the authors' knowledge that has addressed the identification and elicitation of suitable Functional and non-Functional Requirements to use the ToLToB within the context of softwarization for SDP. In the domain of user Requirements Engineering, this phase is significant. Results from it aid the modeling and communication of user-based requirements that are contextually suitable for use (Wu *et al.,* 2016; Curcio *et al.,* 2018). In this paper, we concentrate on the identification of functional and non-functional requirements to use the ToLToB. However, in the User Requirement Engineering process, it is easy for things to go unresolved and as such even supposedly good projects do fail. This happens because of the easy-way-out Fire Brigade or Fighting Approach (Iqbal *et al.,* 2020). Within the context of softwarization, particularly when adopting newer technologies like the blockchain, the absence of a systematic approach that considers the peculiarities of such technology is also responsible for such easy-way-out Fire Brigade or Fighting Approach. This makes it justifiable to have a framework that guides the robust contemplation of requirement issues in advance to tackle this anomaly.

Based on the literature (e.g. Iqbal *et al.,* 2005; Ali *et al.,* 2014; Natsiavas *et al.,* 2018; Oluwatobi *et al.,* 2020; Lo *et al.,* 2020), there is no one-fit-all framework or approach to tackle issues of this nature due to context. Fortunately, despite the non-existence of a one-framework-fit-all approach, a framework can be inspired from an existing framework, and be used in a different context. The consequence of the failure that comes from not paying attention and resolving the issues in any User requirement engineering process can be severe. However, in the context of using the Technology of Blockchain (ToB) for SDP, the level of severity is better imagined than experienced. What is at stake is User's Personal Information. As such, any failure in the attempt to deploy SDP solution would be tantamount to surrendering an entire system for data breach, User Personal Information theft, malicious attacks, etc. Cognizance

of this; this paper presents a User Requirement Engineering framework to systematically identify and elicit Functional and non-Functional requirements as User Requirements to better use the ToLToB to provide OSNSDP. The rest of the paper is structured as follows with Section 2.0 focusing on literature review, Section 3.0 User Personal Information framework as methodology as contribution to User Requirement Engineering to use the technology of Blockchain particularly for Sensitive Data Protection. Finally, the analysis of results from the User Requirement Engineering framework and the conclusion of the paper are presented in Sections 4.0 and 5.0 respectively.

Context of users' requirement for blockchain technology

In this work, requirements and Users' Requirements are used interchangeably, and they are often classified as Functional Requirements and non-Functional Requirements (Kurtanović and Maalej, 2017). Functional Requirements are requirements that specify the set of actions to be performed by a system without considering physical constraints (Mughal *et al.,* 2018). These requirements are statements detailing the services that a system should provide, how the system reacts to inputs and should behave in some particular situations. On the other hand, non-Functional Requirements specify system properties that focus on environmental and implementation constraints. Performance, platform dependencies, maintainability, extensibility, reliability, etc. are other properties that are captured in the nonfunctional requirements specification (Wu *et al.,* 2016). Non-Functional Requirements are goal-oriented requirements, which functionalities seek to compliment system's Functional Requirements with the aim of ensuring that customer needs are satisfied and a software product is delivered within stipulated period and cost.

Users' Requirements are the functional requirements, which a system must fulfill as a matter of system functionality. This system complexity is not complete without the part of the non-functional requirements, which plays a huge role in determining the success of the system. The non-Functional Requirements of a system can be implicit in its users' behaviours. It is thus important to elicit users' requirements from the perspective and context of the user (Goker and Myrhaug, 2008). The motivation to present the proposed systematic user's requirements framework is premise on the non-availability of representative model framework to provide a robust elicitation cum identification context to use the Blockchain technologies for OSNSDP. This is consequent upon the fact that there are issues, which should be resolved to be able to deliver the required benefit of using Blockchain technology for Sensitive Data Protection within the context of OSNs. As found in the literature, users' requirements elicitation and development framework exist to (i) develop ubiquitous computing (Iqbal *et al.,* 2005), (ii) deliver users' views based on usage contexts and involvements in the apps design process to handle the information overload of developers from huge volume of app comments (Oh *et al.,* 2013), (iii) ensure a secure and interoperable data exchange of health related data (Natsiavas *et al.,* 2018), (iv) use smart cards biometrics for the accreditation of voters (Oluwatobi *et al.,* 2020), (v) identify

potential non-functional requirements to leverage federated learning techniques in the face of growing concern for data privacy protection (Lo *et al.,* 2020), etc.

In Iqbal *et al.* (2020), the need to understand users' requirements in global software development was highlighted, while accounting for the benefits of not subscribing to the "fire brigade or fighting" approach to handle users' requirements engineering issues. The process of identifying and specifying functional requirements and non-functional requirements to leverage successfully user's requirements engineering benefits can be understood using best practices from related studies. However, such best practices are yet to be established concerning user's requirements engineering to use the Blockchain technology for OSNSDP. This paper fills this gap by presenting a user's requirements engineering framework to better use the Blockchain technology for OSNSDP.

Taxonomy of the Blockchain Technologies

A good amount of research work has been done in the literature on the taxonomy of blockchain, which outcome is focused on highlighting the features that are essential regarding the areas where the Blockchain technology has and can be exploited (Bellini *et al.,* 2020). Basically, the Blockchain technologies has been and could be used to seek and deploy software solution in dimensions that are known currently and in others that are under contemplation (Gary and Kiayias, 2020). In the literature, the areas where the Blockchain technologies has been successfully applied are known and open (Casino *et al.,* 2018; Zheng *et al.,* 2018; Rouhani and Deters, 2019; Ghosh *et al.,* 2020; Guidi, 2020; Helo and Shamsuzzoha, 2020). In Gary and Kiayias (2020), a taxonomy was presented to serve as a roadmap on how to study consensus challenges in its several guises to apply appropriately the Blockchain technologies. Similarly, in Bellini *et al.* (2020), a concept analysis with Formalism at its core was applied to develop two taxonomies that are relevant in the use of blockchain within the context of distributed reputation and trust management systems.

Other recent research efforts regarding the development of blockchain taxonomies in a bid to learn its use through its categorization for the purpose of softwarization include that of 1) Kumari *et al.* (2020), which work considered possible attacks on unmanned aerial vehicles along with countermeasures. 2) Tonnissen's *et al.* (2020) captured the taxonomy of real-world perspective of different business model lenses and forms with their collaborative influences on token-based economies to help understand start-ups within the context of blockchain. 3) Sai *et al.* (2020) developed a taxonomy using empirically measurable and observable characteristics based on findings from a systematic review of the literature to help learn about the aspect of centralization in the Blockchain technologies. 4.) Ghosh *et al.* (2020), made their research contribution using a survey approach that covered various characteristics of blockchain and its taxonomies to highlight situations, where particular blockchain type should be made functional. 5) Liu's *et al.* (2020) taxonomy focused on the categorization of privacy concerns that are potential treats to OSN image

sharing. 6) Casino *et al.* (2018) work applied a systematic review of the literature with a focus on the disruptive nature of the Blockchain technologies to revolutionize the practice of "business-as-usual" across multiple domains to understand the heterogeneous aspects of blockchain-based solutions.

One of the most comprehensive taxonomies in the literature is the one developed by Zheng *et al.* (2018). This is because it uses a survey technique to give a blockchain taxonomy that introduced consensus algorithms, applications of the Blockchain technologies, discusses the technical challenges and new advances to tackle the challenges with in depth analysis on the future directions regarding the use of the technologies of Blockchain. Despite this depth of treatment given to the possible use of the technologies of Blockchain, existing research work to the best of our knowledge has not captured the perspectives using a Consensus and Business model approach within the context of Softwarization in a single taxonomy. This current paper did this by presenting a taxonomy of the technologies of Blockchain from the perspectives of context of Softwarization. The aim is to situate the context of a software-based solution that is different from the hardware context of approach to use the Blockchain technologies for OSNSDP. The taxonomy developed and presented in this paper is in accordance with the prescription in Nickerson *et al.* (2013) and as applied in Tonnissen *et al.* (2020) about how to develop taxonomies. Going by the provisions in Nickerson *et al.* (2013) and Tonnissen *et al.* (2020), a taxonomy is made up of mutually exclusive categorizations. This mutual exclusivity was represented formally as follows in Equation 1;

$$T_{xmy} = \{ASiP_k, k = 1,\ldots, m | ASiP_k, = \{SiP_{kj}, j = 1,\ldots,nk; nk \geq 2\}\} \quad (1)$$

where

T_{xmy} = *Taxonomy;*

$ASiP_k$ = *Aspects of Situation in Perspective (e.g. a set of dimensions); and*

SiP = Situation in Perspective (e.g. a set of Meta-Characteristics that are mutually exclusive)

By this categorization – taxonomy, the complexities of the Blockchain technologies from the context of Softwarization perspective is thus exemplified to motivate the requirement capture as one of our contribution to research into the use of the Blockchain technologies from the perspective of context of Softwarization.

Related work

The use of Blockchain as a technology to develop trustless systems with enhancement in users' privacy, and other system characteristics such as scalability, interoperability, visibility, latency, audit, etc. is well known in the literature

(Ghosh *et al.,* 2020; Garay and Kiayias, 2020; Bellini *et al.,* 2020). In Esposito *et al.* (2018), the use of the Blockchain technologies to protect data from the healthcare domain was studied with its potential highlighted as capable of economic savings for managing healthcare data and convenience regarding being able to have at real-time patient medical history that are hosted within the cloud. Other contributions regarding the use of the Blockchain technologies in literature include the work of Yang *et al.* (2018), which motivation is spurred by consensus mechanism to develop a deletion scheme that uses the technique of blockchain for deleting data in a Peer-to-Peer (P2P) chain. As part of the research contributions to the use of the Blockchain technologies, Garay *et al.* (2015) and Gervais *et al.* (2016) described the architecture, which could be leveraged to implement consensus and scalable security mechanisms of blockchain in a P2P network. A scheme that applied the Blockchain technologies for privacy preservation with task matching potentials has been developed by WU *et al.* (2019). The scheme was applied within the context of crowdsourcing to identify anonymity with preferences that are consistent between users and their tasks. To forestall a review of lengthy the literature, a summary of related work is therefore presented in Table 1. The review summary is centred around the work that considered requirements as a priority while leveraging the Blockchain technologies for softwarization purpose to solve consensus challenges for business purpose or otherwise.

Table 1: Summary of the literature of related work

Citation	**Requirements**			**TuC - BC**	**For OSN**	**Focus/ GoP**	**Comment**	
	WM	**WGFA**	**WnGA**				**RP**	**LRP**
Rouhani & Deters (2019)	✓	×	×	✓	×	**AC**	×	✓
Arquam *et al.* (2018)	×	×	×	✓	✓	**CtAoI**	✓	×
Truong *et al.* (2019)	✓	×	×	✓	×	**PDP/M**	✓	×
Murimi (2019)	×	×	×	✓	✓	**EPiSNS**	✓	×
Jiang & Zhang (2019)	✓	×	×	✓	✓	**AC&DA**	✓	×
Rahman *et al.* (2020)	×	✓	×	✓	✓	**PMA&AC**	✓	×
Yi *et al.* (2016);	×	×	×	✓	✓	**PPUPM**	✓	×
Wu *et al.* (2019)	✓	×	×	✓	×	**PS&R**	✓	×
Cui *et al.* (2016)	✓	×	×	✓	✓	**PPPM**	✓	×
Joshi *et al.* (2020)	×	×	×	✓	✓	**P&DT**	✓	×

✓ (yes/affirmative); × (no/other nuances of non-affirmative); **WM** (Was Mentioned); **WGFA** (Was Given FULL Attention); **WnGA** (Was not Given Attention); **TuC** (Technology under Consideration); **GoP** (Goal of Paper); **RP** (Research Paper); **LRP** (Literature Review Paper); **AC** (Access Control); **CtAoI** (Check the Authenticity of Information); **PDP/M** (Personal Data Processing/Management); **EPiSNS** (Enhance Privacy in Social Network Sites); **AC&DA** (Access Control & Data Availability); **PMA&AC** (Privacy with Manageable and Auditable Access

Control); **PPUPM** (Privacy Protection for User Profiles Matching); **PS&R** (Privacy, security & Reliability); **P&DT** (privacy & Data Transmission)

Interestingly, as shown from Table 1, most of the work reviewed on the use of the Blockchain technologies in the literature did not consider Requirement Elicitation within the context of Requirement Engineering. Additionally, though Blockchain is highlighted as technology with wide recognition in providing solution for sundry privacy interests, requirement concerns were not given adequate attention. The work of Rahman *et al.* (2020) gave full attention to requirement concern in their use of Access Control List to ensure that the privacy challenges of protecting users' sensitive information are protect in a Distributed OSN (DOSN). With the Access Control List, they achieved an auditable and manageable access control framework that uses the Blockchain technologies and can define privacy policies. Our work differs from that of Rahman *et al.* (2020) because of its focus, which is to present a Requirements Engineering framework to enable the use of the ToLToB to provide OSNSDP within the context of softwarization. In contrast, this work exploited the trustless potentials of blockchain to present implementable requirements. Hence, the consensus mechanism of the blockchain was fully exploited, unlike in work of Rahman *et al.* (2020). Also not oblivious of the fact that in the context of businesses where privacy concerns are dynamic, to ensure the provision of a most useful solution within the context of softwarization, the business model perspective was included in the taxonomy presented to help understand the privacy concerns in the protection of online sensitive data. By this, we believe the requirement provision effort of Rahman *et al.* (2020) is extended by the provision of more requirements, which application were demonstrated through the provision of user and attacker scenarios to highlight appropriate usage situations from the perspective of end users.

It is significant to give adequate consideration to Requirement Elicitation when setting up a system. And for OSNSDP, there is the absence of a framework to guide Requirement Elicitation. Motivated by this absence of a Requirement Engineering framework for Requirement Elicitation to use the Blockchain, this paper makes the contribution presented herein. The contribution in this work is significant in that though there are research work in the literature that attempt the provision of requirement (e.g. Rouhani and Deters, 2019; Truong *et al.,* 2019; Wu *et al.,* 2019), they were not explicit, tailored and captured in such a way that their provision is systematic to guide the use of the Blockchain technologies. Though the attempts in Nasim and Buchegger (2014) and Rahman *et al.* (2020) are explicit, the provision made regarding requirements is not sufficient to build a framework to guide Requirement Elicitation to use the Blockchain technologies.

Materials and methods

The framework in Figure 1 is a four-step framework, which doubles as the methodology adopted for this work and presented as our contribution to research in users' requirement engineering for Requirement Elicitation to use the Blockchain technologies. Each of the steps focuses on a methodological stake that provide procedural contemplations that are suitable to guide the elicitation and development of usable requirements as far as the use of the Blockchain technologies is concerned. The four steps of this framework are visible at its Left-Hand Side (LHS) (see Figure 1). Similarly, the expected outcomes are represented as shown at the Right-Hand Side (RHS) of the framework (see Figure 1). In its application, a casual effect, which emphasis and focus is on the elicitation and development of usable requirements should be expected. When it does, the effect seeks a true representation of the system stakeholders' perspective. This effect/outcome would support a substitute design. A design, which could guide a system's ultimate implementation not only in the context of using the Blockchain technology but in other software requirement engineering contexts.

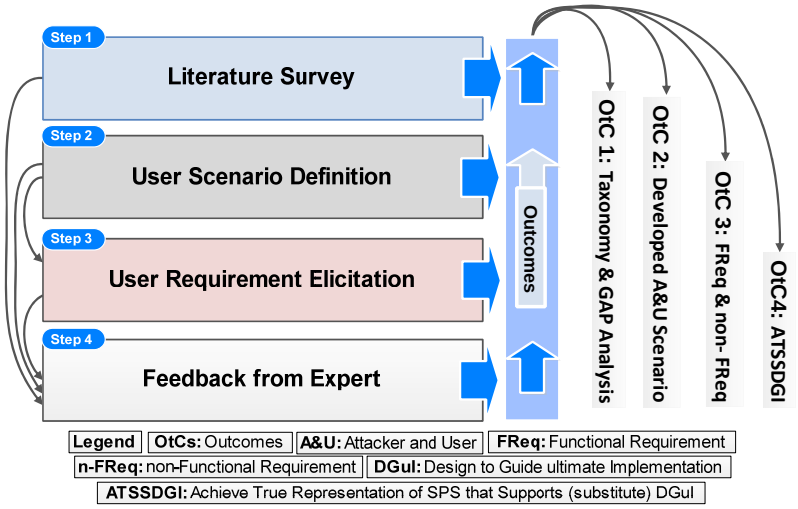

Figure 1: Requirement engineering framework

User requirement framework to use Blockchain technology

Research efforts in the literature have shown why and how software projects with so much significance end up failing (Goguen and Linde, 1993; Iqbal *et al.,* 2020). The consensus about this is that such failures result from the wrong (or inadequate) use and handling of requirements. The attempt to use the Blockchain technologies for SDP, which is occasioned by the finding that the bane of SDP on OSN is the centralized nature of the architecture on which OSN is

implemented is no exception. The use of the Blockchain technologies as a good decentralization mechanism to offer a software solution within the context of softwarization would therefore require the right handling of requirements to use it. The first and important step, which is the main aim of this work, is the provision of a Requirement Engineering Framework. Requirement Engineering is therefore necessary for a nascent technology to guide the Requirement Elicitation of appropriate requirements to offer software-oriented solution to use the Blockchain technologies to achieve SDP. To realise this goal, the operational setting of OSN, which data is to be protected is considered. This is because of the fluxing nature of the OSN Environment, which influence is evident on the sensitive nature of the data. The relationship between the OSN environment as a whole and the control exerted by the social, cultural, and political dynamics of the users who engage in myriads of interactions and online transactions within the social media space are also taken seriously.

Given the unwavering influences on the OSN environment and the volume of sundry users in this environment, it is important to identify the right requirements that captures the perspective of diverse users and the context of social, cultural, and political dynamics. To ensure OSN data privacy in the context of SDP, our proposed framework becomes central. This is because of the guide it provides in the identification exercise to determine the requirements that are fitting to use of Blockchain technologies. Cognizant of this backdrop, the framework presented in Figure 1 provides a four step inter-relational approach as highlighted with the arrows at the LHS of the framework. Additionally, the arrows at the RHS depicts the outcomes from the aggregate of activities to be carried out in each of the four pillars - steps that make up the framework. These details are presented as follows.

Step 1 - Literature survey

Usually, the requirements from the users that the system must be built around are readily not available. Interestingly, these requirements are needed since they are replicates of users' personas, which can serve as design vehicles to keep designers on track during system design and implementation. This informs why it is significant to elicit these requirements properly. The context that influences the system and its boundaries, etc. are to be considered in defining system requirements (Pohl and Rupp, 2015). This is why the fluxing nature of OSN environment and its social, cultural, and political dynamics were considered as stated earlier. In this phase, sufficient literature survey is needed (as done in this work) to systematically capture user requirements as an aggregated endeavour. This phase is important due to the critical role of the review of literature in that when successfully synthesized with the absence of data, new theories and frameworks are generated. As an unrefuted evidence that is born out of the state-of-the-art; it is so foundational such that it makes science remain a cumulative endeavor (Pare and Kitsiou, 2017). This theoretic occasioned the inclusion of the survey of literature in the framework (see Figure 1) to provide aggregated review. The

essence is to engender and re-enforce rigorous and systematic scientific strategy to identify requirements. This helped in defining evidence-based eligibility criteria to validate identified requirements. This was achieved through a set of activities that was performed in the Requirement Elicitation Process under this phase. It was necessary to perform these activities to pin point any missing aspect in Requirement Elicitation Process peradventure there was any. There were no missing activities in Requirement Elicitation Process in this work, may be because of the Blockchain technologies context that is under consideration. However, this may not be the case in another context. This is because the framework provided to guide these activities as highlighted in Wong *et al.* (2017) which when applied is capable of vigorously leading the way to perform the activities such that any missing aspect is easily identified and improved on during the Requirement Elicitation Process. The set of activities in the framework as presented in Wong *et al.* (2017) were extended based on findings in Natsiavas *et al.* (2018) and Iqbal *et al.* (2020) to guide the Requirement Elicitation Process under this survey phase. These extended albeit a set of fine-grained activities are shown in Figure 2. The most significant outcome in this step is the taxonomy and gap results, which are available in the Section on result.

Step 2: User scenario definition

As is, the expectation in this work is to deploy the technologies of Blockchain to provide SDP within the context of OSN. The interacting elements within the context of the theme and objective of study are to be considered. In this study, OSN environment are made the milieu of consideration and the foregoing the objective in question. As a result, the users of the proposed system of SDP aside from devices and apps become key players in the OSN environment. In the OSN environment, users identity based on the digital traces they leave behind after every interaction are visible. This makes it possible to track the combination of users' task-orientation and social dynamicity in the OSN space. These combinations are imperatives that makes the notion of usability in this instance important, but not as relevant as Interactivity and User Experience Goals in the steps required towards Requirement Elicitation. Therefore, to achieve SDP with Blockchain technologies and within the context of Softwarization, it was important to focus on eliciting requirements that will drive the development of SDP-oriented solution that will deliver Interactivity and User Experience Goals. The influence of social, cultural, and political dynamics not undermined here since the data to be secured are users' sensitive personal data. The need to understand the actors that are involved in the context of SDP therefore became overarching. Hence, the focus on two actors - the user whose data is to be protected and the attacker who must be stopped from maliciously attacking user data.

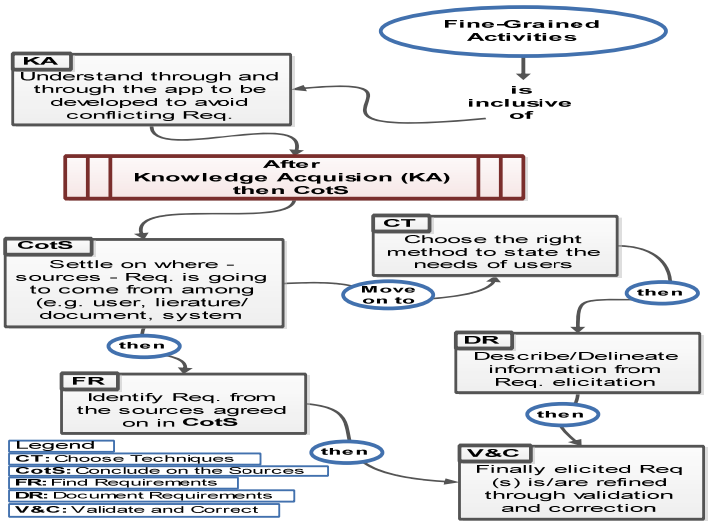

Figure 2: The fine-grained activity and its inclusiveness.

Since what we seek is a software solution and not that of hardware (i.e. softwarization), the computing context where the SDP mechanism will be deployed remained a secondary concern that is out of the scope of this work unlike the forgoing. Detailed narratives of both actors are to be known through appropriate representation. This was best represented using the scenario approach, which technique allowed the presentation of useful narratives about the actors. As such, corroborative and realistic situations regarding actors' behaviour during interactions (on the part of legitimate users and attacker) were given utmost attention. In this paper, while the scenario of occurrence of SDP is formally specified as shown in Equation 2 to 3, the actors and their scenarios were defined.

The practice here aids the easy translation of scenarios into fitting personas and then into believable characters. As a user-centred design methodology, these scenario-based approaches relied on factual/scenario development to encourage character believability. Thus, persona as explained in Lopez-Lorca *et al.* (2014) that scenarios may be textual delineations but they resonate usage situations that are from end users' perspective. This makes the design of technology stress-free since there are defining property using the scenario projections to create concrete terms of activities that aggregately show possible engagements when users perform tasks. By this purported design, implications are easily inferred from functional and non-functional requirements. In this work, the user as a key element of a scenario's property doubles as both victim and attacker. In concrete terms of activities, the user type - victim and attacker and other elements were appropriately modelled as shown in Equation (1). In this paper, the assumption is that users' need their sensitive data to be protected to encourage privacy. Here, also we assumed scenarios (or forms) are narratives of expectations that causes or alleviate privacy breach. This semblance of expected

system functionalities were formulated for SDP. Expected system functionalities were delineated to be facilitations, which operations are invoke-able to offer protection from actors (likely victims) during interactions on any OSN.

For more effectiveness, in formulating expected system functionalities, the principles of how attackers operate as x-rayed in Natsiavas *et al.* (2018) is considered. This resulted in employing the users' personal information to match possible users' scenario, which may be different from scenario to scenario since context and functional requirements majorly decides this. Given that the SDP scenario is (*sd*); a *6-tuple* applied is formally defined it follows (see Equation 1);

$$sd = \{u, sa, ea, ld, fra, \beta\} \quad (1)$$

where

u = User (set of victim & attacker)

sa = Sensitive data

ea = Encryption algorithms

ld = Local database

fra = Friend recommendation algorithm

β = Blockchain that is based on Hyper-ledger Indy framework

Additionally, the Blockchain represented as *β* is conceptualised as a *3-tuple,* which is presented as follows in Equation 2 as follows;

$$\beta = \{cc, cm, s^1e\} \quad (2)$$

where

cc = Chain-code

cm = Consensus mechanism

s^1e= *Hashed of the encrypted data*

In this paper, the scenario method satisfied the need to provide a check mechanism to help minimize the biases that often occur because of too much subjectivity in a typical Requirement Elicitation Process, particularly in the literature survey phase. The five-step fine grained activities in Figure 2 and now the use of the scenario method should both contribute to minimize the measure of bias in the Requirement Elicitation Process as observed in this work starting from the literature review phase and now the scenario definition phase .

Step 3: Eliciting user requirement

Poorly designed systems are often detraction. This implies that stakeholders are prevented from rewarding expected user experiences. This is the phase (or step) where efforts are made to avoid this. Correctly eliciting requirements from the right source and real users, which is part of the activities shown in Figure 2 is a key step in this direction. Expected user experiences are derived system functionalities that users want to see and experience when using a system (Lopez-Lorca *et al.,* 2014). For maximum impact, users' Requirement Elicitation with stakeholder centredness were motivated here by including personal values. As Proynova *et al.* (2011) hinted; user requirements are hidden and may be uncovered when stakeholders' personal values are included in the elicitation phase. To do this, inputs from stakeholders who are less technical are game changers at this point. Users' context to leverage the use of the Blockchain technologies for SDP are part of these inputs and include the context of prospects, potential risks, and other challenges with the use of blockchain. By sufficiently x-raying these in the light of requirement elicitation, the know-how to make informed decisions on issues of blockchain adoption, in this case for SDP in the OSN environment was achieved.

There may be ambiguities in the delimitation of user requirement elicitation. This usually happens because of the dynamics in users' personal information. Approaches found in Wong's *et al.* (2017) and Natsiavas' *et al.* (2018) were useful in this regard to uncover appropriate system needs and conclude on what goals (i.e. Functional requirements) to adhere to. High-level goals that reflect users' needs were easily complemented by abstract (or non-Functional Requirements) user requirements. As part of the outcomes specified and expected from the use of the framework in Figure 1; the Functional Requirements and non-Functional Requirements were meant to serve as baseline functionalities of a proposed system. Very importantly, this implies that users' tasks were associated with the right operations and at the same time with the right actors to avoid the user (but attacker). Proper system specification could make these functionalities come alive. The absence of usable scenarios (narratives) of both actors would make this difficult to achieve. Since OSN data is sensitive, and it is what is at stake; in this phase, a Threat Analysis may be introduced to ascertain the measure of vulnerability that exists and needs to be mitigated. The alternative is to present a gap analysis result, which is what was opted for in this work (Natsiavas *et al.,* 2018). Threat Analysis when applied; aside from considering the technical aspect of vulnerability, would also shed light on the legal, functional, political, and personal aspects as with the gap approach to deal with SDP of OSN data.

Step 4: Feedback from expert

In this step, salient concepts, which may not usually come to the fore at the earlier steps are considered and discussed with experts. This could happen within a research team, as was the case in this paper. For a more elaborate project, a team of expert can be put together. Outputs (or outcomes) from the framework in Figures 1 and 2 are reviewed. By

this review, an obvious contrast of OSN as per SDP as-is - current state without the introduction of the Blockchain technologies and to-be - the state after applying the Blockchain technologies is expected as gap result as envisaged from step 1. Arriving at this out shows that the ideas presented using the Requirement Engineering framework in Figure 1 have been re-evaluated and the resultant concepts are re-codeable to reflect emerging set of requirements. How users perform tasks (i.e. work) in this case users' interaction on OSN in this current work were identified as observed for brainstorming amidst detailed review. Inputs from survey and workshop if affordable, particularly for large projects that are funded unlike this current one could be included. Expert feedback and few user interview going by the practices in Ahn and Chong (2006), Natsiavas *et al.* (2018), Mindila *et al.* (2019), and Iqbal *et al.* (2020) could also be incorporated.

In this paper, expert feedback methodology within the context of the Delphi technique with brainstorming based on the 50% rule as shown in Iqbal *et al.* (2020) was applied in this phase to obtain expected requirements. What obtains in literature is the use of one or more of these methods to collect new requirements (Ahn and Chong, 2006; Natsiavas *et al.,* 2018). By using these approaches, relevant stakeholders' engagements are validated as expected outcome going by the proposed model framework (see Figure 1). Based on the 50% rule, 50% of the experts that were involved in the feedback process supported opinions that correspond to requirements. On ascertaining this, the resultant requirements were accepted following what obtains in similar studies (Cox *et al.,* 2009; Iqbal *et al.,* 2020).

Results and Discussion

This section is dedicated to the presentation and analysis of the outcomes of the methodology (see Figure 1) that was applied in this paper. Going by the diverse activities of Requirement Elicitation Process performed within the context of this work, it was necessary to focus on the important outcomes

Outcome from step 1

There are two outcomes from the survey activities that happened at the literature survey step of the framework. The outcomes are the taxonomy in Figure 3 and the gap analysis result that are presented as follows.

Taxonomy

The taxonomy presented in Figure 3 highlights the perspective of *Consensus* mechanism and *Business* model process within the context of *Softwarization* (CBS). This taxonomy resulted from the survey of the literature and the supporting activities that were performed. The taxonomy is consistent with the provisions in Garay and Kiayias (2020), Kumari *et al.* (2020), and Tonnissen *et al.* (2020). The CBS perspectives stems from the need to understand

the concept of the mechanism of unanimity - consensus, which successful handling within the context of softwarization seeks to help the potential creation of values using business model process. Achieving this unanimity (i.e. consensus) was found to be possible as affirmed by the report in Zheng *et al.* (2018) and Garay and Kiayias (2020). Rather than a hardware solution, a software solution is identified as capable of mitigating the challenges of centralization using a distributed mechanism. Hence, the need to rethink this solution. Going by the way of business model processes, this rethinking in this current work yielded two contrasting states. 1.) The state of OSN regarding SDP without changes (i.e. as – is), and 2.) The futuristic state when the Blockchain technologies using anonymity (or consensus strategy) is introduced and thus depicts improvement and inclusion of change (i.e. the state of to – be). These are summarized in the taxonomy in Figure 3. This allows the conceptualizations that emphasizes the technical conceptions that are to be pursued in relation to the use of the Blockchain Technology. The scope of pursuance of this as it relates to SDP is aggregately scoped using the taxonomy in Figure 3. The taxonomy serves a guidance to provide the leverage to create the structure wherein relationships that are useful and exists between the diverse entities involved in SDP with codifiable facts are described.

The requirement captured and addressed in this paper is platform-based. Therefore, as observed that OSN run on business models. This implies that the enforcement of anonymity using the consensus mechanism is meant to create values in the OSN virtual space (Han *et al.,* 2018). The customer-centric business models OSN run on are made up of diverse actors. These actors are engaged in multi-level layer interaction. This makes it imperative to think digital solutions for SDP that stimulate value creation. Within the contexts of value creation, it is important as observed to broadcast functionalities securely in ways that are oblivious to attackers.

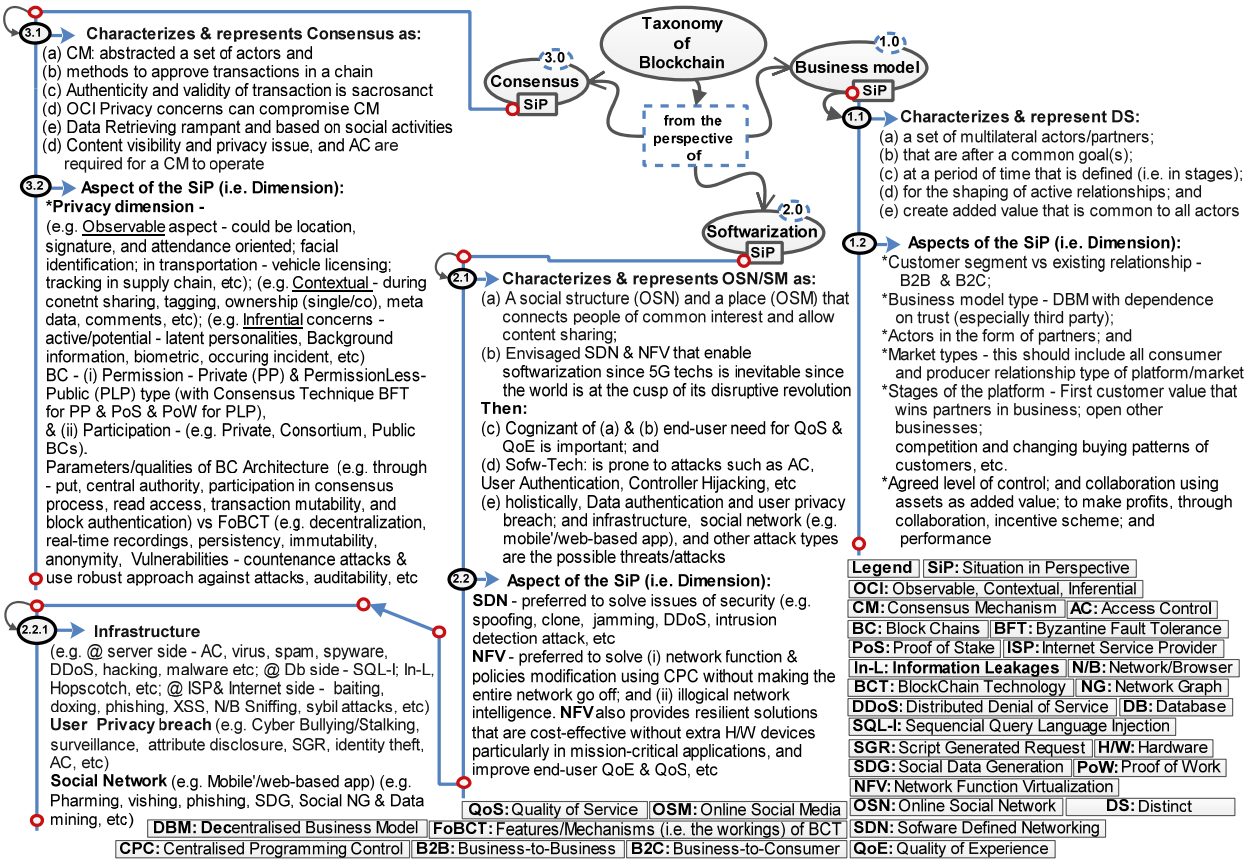

Figure 3: Taxonomy of blockchain from CBS perspective.

This finding is consistent with what obtained in Krcmar and Hein (2020) and Tonnissen *et al.*, (2020), which highlighted the imperative of digital solutions to stimulate value creation. In their case, the mechanism to enforce governance control is needed to organize multi-level layer interaction in favour of users rather than in favor of the service providers or platform owners. This level of governance was observed to be lower and capable of attracting variety of business models. This is consequent also upon being able to accomplish decentralization such that dependence on third party concerns is of little or no consequence. This observation is also upheld and supported by the postulations in Kumari *et al.* (2020) and Tonnissen *et al.* (2020) in the context of softwarization. The taxonomy in Figure 3 will be useful to inform developers about strategic guidance. This will happen through the many classifications summarized into the taxonomy to address issues in their many guises from the Context of

Softwarization perspectives. Probable operations in various settings can also be inferred from the taxonomy, which is diagrammatically shown in Figure 3.

Gap result

The gap result presented in Figure 1 is inferred from the taxonomy in Figure 3. Its conclusive assertion rely on the Desk based research that entailed the reviewing of materials that included published papers in scientific journals and conferences. This took place in the first step of the proposed framework. The outcome of the Desk based research is the taxonomy and then the summarized gap result presented in Figure 4. What is particularly significant in the summarized gap result is the criteria applied to measure/analyze the gap. The criteria provided the standard to both show the depth of the coverage of the taxonomy and the qualitative differences between the target - future state and the current state of OSNSDP. The current state in the diagram (see Figure 4) tells of where "we are and moving out of" due to the many research going on to change things regarding OSNSDP (Beigi and Liu, 2020), and "where we should be (i.e. the future state)." Based on the CBS criteria, the comparison in the presentation in Figure 4 shows the existence of gaps between the current and future state of OSNSDP. Regarding this, the gaps highlight the absence of (i) anonymity (i.e. the non-support for Consensus interactions), (ii) value creation (i.e. the non-support for sundry Business models) since sensitive data must be protected, and (iii) support for softwarization (i.e. satisfy all the requirements that make the contemplated solution software-based).

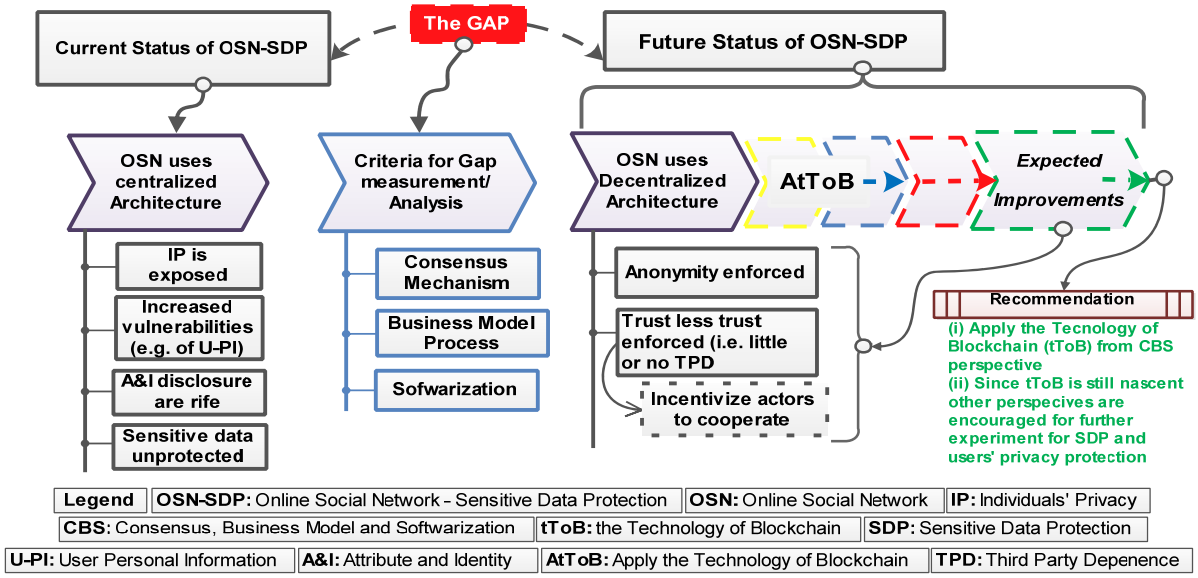

Figure 4: Summarized Gap Result.

Outcome from Step 2

The activities carried out in step 2 based on user scenario definition are meant to develop appropriate attacker and user scenarios. These scenarios are presented in subsections 4.2.1 and 4.2.2 as follows

Scenarios of OSN user and attacker

The result in Table 1 is a sample of the scenarios of both a possible attacker - who is also a user on the OSN platform and users who are not attackers. The scenario were conceived drawing on and using the Desk Based Research (i.e. review) approach as done in Natsiavas *et al.* (2018), hence the citation in the table.

Table 2: Sample attacker and user scenarios.

<table>
<tr><th colspan="2">Sample Attacker Scenarios</th><th>Citation</th></tr>
<tr><td>S. S (1):
Attackers rely on “baiting” to stimulate victim’s (targeted users’) curiosity. Then attackers wait (i) for targeted users’ interest to be raised, (ii) for their victim to take the first step and initiate contact.
In this baiting, an attacker may assume and use a persona that seem attractive to a victim with the belief that the victim will be encouraged to establish contact.
<u>Comment</u>
In this approach, there is no room for direct contact else suspicion might be raised in users.</td><td>Scenario (2):
In this scenario, an attacker made his/her phone number available to the target users. The attacker had earlier spoofed by way of exploiting users in three dimensions through their features (i.e. user personal information, behavior and content). Persuasive means are also employed by attackers who pose as trusted and known entity to targeted users.
<u>Comment</u>
Here attackers are patient and certain that (i.e. proposed victims) will commit themselves</td><td>Irani et al. (2011); Aiello and Ruffo (2012); Zhou and Chen (2020);</td></tr>
<tr><td colspan="2"><u>H.S (3):</u>
Targeted-victim attack; Random-victim attack; Seed-targeting attack; Distant-seed attack; & Neighborhood and/or Friendship attack scenarios could be multiple scenarios in the arsenal of a single attacker as presented below:
<u>Targeted-victim attack scenario:</u>
Here attackers establish attack with targeting users that they have some mutual friends/relationship.
<u>Random-victim attack scenario:</u> The attack in this scenario is regardless of the existence of friendship/relationship between a target user & attacker. And this happens as attackers establishes attack with target user randomly.
<u>Seed-targeting attack scenario:</u>
Here experienced attacker preys on the users, which OSNs operators’ trusts.
<u>Distant-seed attack:</u>
This attack is on a random trusted users, which becomes vulnerable since attackers successfully become friends with users on the particular OSN (Zhou and Chen, 2020).
<u>Neighborhood and/or Friendship attack:</u>
Here attackers use what they know (knowledge) about victim’s neighbours to re-identify them</td><td>Zhou and Pei (2008); Tai et al. (2011); Schillinger and Schindelhauer (2020).</td></tr>
<tr><td colspan="2"><u>Sample User Scenario</u></td><td></td></tr>
</table>

User Scenario: Users do demonstrate behaviours that are incautious. Level of human interaction, which in some cases make interacting parties solve puzzles is also possible. These behaviors can be inducing when attackers' requests for contacts, etc. When granted harm can be done. Users are vulnerably by their innocent behaviours. They therefore become easy target and so are easily tricked to grant access to attackers. When unsuspecting users grant access to attackers, portion of their private information are inevitably disclosed and they ultimately become victims. The extent to which this happens is proportional to the level of trust targeted users place on their new friend. Invariable, a user identifier in an OSN is already know in real life to attackers, who inevitable introduces self with false personas. This happens in the social contexts of OSNs. Users desire to be interactive. There is the belief of being_interactive with peers that are highly trusted. This brings/leads users to become victims, and high quantity of their personal information are disclosed. Comment In the user scenario, six features are likely to make OSN users victims of one form of attacker or the other. These features in three dimensions falls into three dimensional perspective: (i) User personal information (e.g. *the number of friends, and user age*); (ii) User behavior (e.g. *the frequency of access, and the frequency of updates*); and (iii) User content of message (e.g. *the number of comments, and URL ratio*)	Aiello and Ruffo, (2012); Zhou and Chen (2020)

The findings highlighted in Table 2 foreground the possibilities, which are to be given attention at the level of requirements when contemplating implementable solution. For instance, consistent with the postulations in Zhou and Chen (2020), the scenarios of attackers include the exhibition of imposture role to compromise in a serious circumstance users' security in the context of OSN. This imposter role enable them to intelligently mimic the behaviour of users on a normal circumstance to move their true identity out of sight. The plausibility of the understanding adducible from the scenarios reported in Table 2 is in the alert level of sensitivity that tell of the tune to which OSNSDP mechanism is implied from them (i.e. attackers being able to mutate to 1) become friends with real users, and 2) becomes friend directly with a subgroup of users that are trusted. By implication, a situation where the target user and the attacker is allowed to have same friends in common, which must not be discountenanced by solution provides. This knowledge is important because this can be the scenario in several network platforms, where attackers achieve this feat randomly. In Zhou and Chen (2020), this was acknowledged by alluding to the possibility of existing scenarios where users that are trusted by OSN operators are known and their characteristics learned by skillful attackers. These scenarios and the archetypal scenarios presented in section 4.2.2 can be further analyzed using appropriate models, which is beyond the scope of this current work. Such analysis though, still helps to narrow

down to a thorough fine-grained level of numerous possible scenarios of vulnerable OSN services for which extra mechanisms of protection are to be provided to secure online data across the network platforms.

Archetypal user scenario

The narrative in Table 2 in the context of this paper is consistent with the practice in Moeckel (2018), Zhou and Chen (2020), and Schillinger and Schindelhauer (2020) to mention a few. The scenarios archetypically focus on three possible attacker scenarios with narratives about how targeted users are baited and become victims within the context of OSN. They put possible attackers' and users' personas in the context of the action(s) that is expected of them as attackers and target users. The provision in Table 2 uphold the postulations in Moeckel (2018) that this context would remain a key aspect of persona's creation before proposed system implementation. Based on the Desk based research adopted in this work, it was found that it was important to find a ground to build attackers' personas. This is the relevance of the scenario(s) created in Table 2, which relied on the framework developed by Moeckel (2018). With this framework, embodying the personas of developers was easily avoided to favour real users. This pursuit is needed for social systems (e.g. OSN and domestic systems). Consistent with what obtains in Lopez-Lorca *et al.* (2014), the right personalities using appropriate narratives are enforceable from the scenarios in Table 2. It was found that personas represent archetypical users (e.g. as victims or attackers). Such scenarios are task-specific and describe the activities of users as victims or attackers and what make them vulnerable (as victims) or lethal (as attackers).

Within the limited scope of this paper, the focus was on scenarios and not personas. However, the deviation to personas was to show the relationship that exists between scenarios and personas. Scenarios are suitable for the aim and interest of this paper, which is on requirement capture (i.e. elicitation) and not implementation. For example, the emphasis of the narratives in a scenario is on specific attacks as shown in Table 2. This by implication means that an attacker persona may have several scenarios (attacks) that are likely to change eventually as time goes on, thus supporting the claim in Moeckel (2018) and Zhou and Chen (2020). The narratives in the Table 2 briefly highlights the activities of attackers by which they can easily swoop on their victims. The features of users also highlight the functional activities that makes them vulnerable. These deducible narratives serve as springboard during design. As presented in Tables 3 and 4, the scenarios presented inspired the Functional Requirements and non-Functional Requirements shown as deducible narratives to use the Technology of Blockchain to deal with privacy concerns that hinge on confidentiality. The confidentialities under consideration were found to be different. This implied that the solution is access management particularly to protected resources, which is where Blockchain technologies comes in. In Aiello and Ruffo (2012), this move was highlighted as capable of assuring full privacy during interactive activities.

Outcome from step 3 – user requirement elicitation

The requirements presented in Table 3 are not only going to be useful to handle access control issues regarding privacy matters as attended to in Rahman *et al.* (2020), which helped to contrasts this current work regarding requirement elicitation like others (e.g. Garay and Kiayias, 2020; Kumari *et al.*, 2020) that approach their work from the perspective of taxonomy. This current work highlights other aspects such as the mitigation of attack on OSN users' privacy and support for protection of sensitive data that is rife in OSN through Users' Personal Information, attributes and identity disclosures. The novelty in the requirements presented in Tables 3 and 4 is in their usefulness to ensure the enforcement of anonymity in such a way that actors (users) are not incentivize to cooperate during interactions. Imposture role are bait-oriented and they lure users during interaction. With these functional and non-functional requirements, the possibility of flexibly allowing individual users to engage others during interaction with their own different operational permissions will be precluded. The belief here is that the proposed requirements in Tables 3 and 4 would find usefulness in implementing irrevocable policies as postulated in Rahman *et al.* (2020) using implementable Blockchain technologies solutions to enforce sensitive data protection on OSN. The authors in this current work are of the opinion that if the foregoing flexibilities are permitted, attackers would mimic a genuine user. This could happen whenever imposters are able to lay their hands on user's personal information, attribute and other sensitive identities to compromise supposed genuine transactions online.

Table 3: Elicited functional requirements.

FRID	Requirement Descriptions
FR1	The system should be able to allow user to register and create a profile
FR2	The system should allow only registered user to login and logout
FR3	The system should allow registered user to edit their profile
FR4	The system should allow registered user to set a profile picture
FR5	The system should allow registered user to reset their password using the " Forget Password"
FR6	The system should allow registered user to search for new friends
FR7	The system should allow registered user to create/reply/edit/delete/share a post(s)
FR8	The system should allow registered user to follow/unfollow a friends
FR9	The system should allow registered user to viewing other user's profile
FR10	The system should allow registered user to assign visibility permission to friend (✓ Private: Only the user and friends can sees their posts. ✓ Public: Everyone can see the posts theoretically if they visit the user's profile, but only followers (both approved and unapproved) see the user's posts in their feed. ✓ Approved-Followers: Only those followers, whose follow requests have been approved by the followee can see the followee's posts.
FR11	The system should allow registered user to like/dislike a post
	The system should allow registered user to choose a node role (i.e. validator or observer node
FR12	The system should allow registered user to accept a friend
FR13	The system should allow registered user to send friend request

FR14	The system should allow registered user to search for a friend
FR15	The system should allow registered user to generate and send a private key for other friends to view their posts
FR16	The system should allow registered users to upload to files (video, audio, pictures, pdf)
FR17	The system should allow guest user to search and view basic information about a registered user and send a message to them
FR18	The system should allow the DApps to display friend list using the friend recommendation algorithm
FR19	The system should allow the DApps to send confirmation to user email to validate newly registered user.
FR20	The system should allow validator nodes to vote to elect a leader using consensus protocol in the Hyper-ledger Indy Blockchain
FR21	The system should allow the encrypted and hashed transactions to be stored in the Hyper-ledger Indy Blockchain and replicated to all the nodes in the network

FRID (Functional Requirements ID); **FR** (Functional Requirements)

The possibility of decentralizing OSNs has made it imperative to seek new requirements to implement and ensure that the decentralization is enforced to accommodate sufficient anonymity when users are engaging the system. This implies that control to a large extent is relaxed at the end of service providers and strengthened at the user end. The requirements suggested in Tables 3 and 4 can contribute to making the existing central authority redundant. As much as possible for this purpose, the requirements have been presented as fine-grained and implementable requirements that are user-friendly to manage the attribute profile and privacy concerns of users. The authors are optimistic that their use will help fulfill the requirement for SDP. By it (i.e. the requirements), developers will be to tackle the challenge at hand and present a solution that mitigates leakage disclosures that are capable of compromising users' privacy. These proposals are consistent with the dealings and result in Beigi and Liu (2020) and Rahman *et al.* (2020), etc.

Table 4: Elicited non-functional Requirements.

Types of Non-functional Requirements	**NFRID**	**Description of non-functional requirements**
Usability Requirements	NFR1	The system should be available online at all times to users
	NFR2	The system should be presentable on low-resolution devices (mobiles and tablets).
	NFR3	The system should be easy to learn and usable by both sophisticated and novice users
	NFR4	The system should respond to user's activities quickly
	NFR5	The system should provide conveniences of usage
	NFR6	The system shall be accessible to all registered participants
	NFR7	The system should be fast in operation
	NFR8	The system must have a standard and friendly Graphical User Interface (GUI) that allows data entry, editing, and deleting of data during processing with ease

Performance Requirements	NFR9	The system should allow reliable storage of information
	NFR10	Posts should be placed in the right category for quick response by users
Operational Requirements	NFR11	The system should be easy to maintain and upgradable
	NFR12	The system should be able to work with relevant hardware devices
	NFR13	The system should not be prone to crashing and errors.
	NFR14	The system should be able to handle and cater for multiple users
Security Requirements	NFR15	The system should allow registered users to has access to posts according to their visibility permission
	NFR16	The system should ensure sensitive information is hidden from non-users and other unauthorized users
	NFR17	The system should allow Password to be case sensitive.
	NFR18	The system should allow only registered users to use the system
	NFR19	If anyone send a message, the user should able to know if it is a guest user or a friend in the network.
	NFR20	Personal information of users should be protected
Portability Requirements	NFR21	The system should be compatible to all operating systems and hardware
	NFR22	The system should operate on demand
	NFR23	The system should be compatible across browsers
Space Requirements	NFR24	The system should not consume much space
Ethical requirements	NFR25	The system should comply with quality assurance and other regulatory standards
	NFR26	The system allows the removal of malicious nodes

***NFRID** (Non-Functional Requirements ID); N**FR** (Non-Functional Requirements)

Outcome from step 4 - feedback from expert

The major outcome from the activities performed in this step is the knowledge of the wherewithal to achieve the True Representation of Stakeholders' Perspective of OSNSDP System (TRoSPOS). This wherewithal is about how developers should contemplate attacker personas and put them into action. As concluded in Moeckel (2018), this representation makes it easy to determine the true representation of functional and non-functional requirements. However, to get to this point, based on expert recommendation, archetypal users' behaviour in nefarious ways that are possible are first captured. Following the recommendation in Moeckel (2020), a third dimension (i.e. level) of TRoSPOS is presented. The others are already presented in two levels: the taxonomy and scenario with a little bit of personas. This entailed the profiling of attacker. It demonstrates attacker-centric thinking that is capable of serving as a baseline to help design against the group of fraudsters/people by visualising existing knowledge to compare patterns of genuine customer behaviour and malicious attacker behaviour.

The importance of this true representation is the unveiling of a representation of how determined attackers are. This dimension of new profiling gives insights that are valuable to understand what motivate attackers, awaken and sustain their determination. This is important to inspire appropriate defense mechanism, which is found to be consistent with the postulation in Moeckel (2020) that knowing those behind online attacks would help recognize how far the attackers will go. Cognizant of this, the expert recommendation resulted in three levels of attackers, which finding support the conclusions in Moeckel (2018; 2020) as shown in Figure 5. It was also discovered that area, context or location of operation in the cyber space determines how these levels of attackers act/behave.

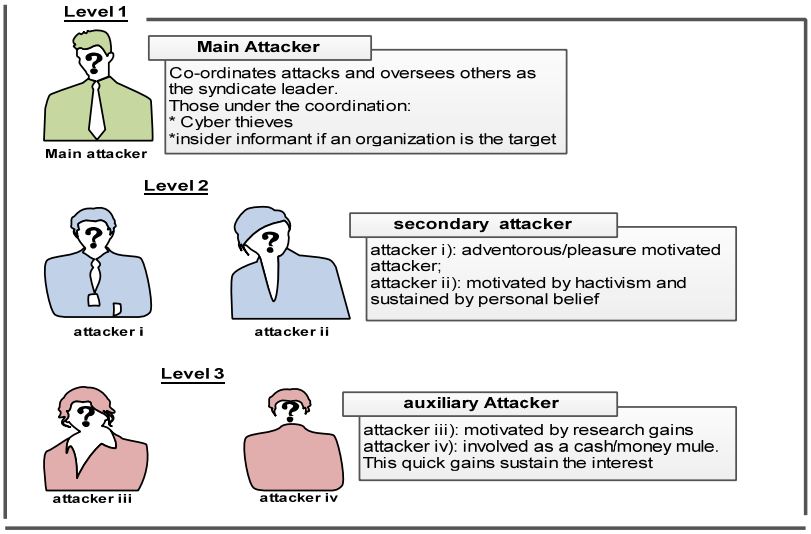

Figure 5: Example profiling of possible attackers.

Conclusion

The main motivation for this paper stems from the belief that privacy and trust concerns are enforce-able with the Theoretic of Leveraging the Technology of Blockchain (ToLToB) to give users complete control over their data even among untrusted peers on OSNs. In this age and time, when attackers have found OSNs as a target of profitable reward (Koll *et al.*, 2017), it is imperative to mitigate their attacks on unsuspecting users of OSN platforms. The common threats within the context of OSN are spoofing, repudiation, tampering, information disclosure, elevation of privilege, and denial of service, and other unforeseen threats as highlighted in the Taxonomy shown in Figure 1 and from Context of Softwarization perspective. In the context of this work, the successful use of the Blockchain technology with appropriate Functional and nonfunctional requirements would result in a software solution that is able to manage sundry threats. To the best of the authors' knowledge, this is the first study that systematically

presents and apply user requirements engineering methodology that provides a comprehensive view like ours. A user requirements engineering framework was proposed and applied to elicit functional and nonfunctional requirements that are re-useable to develop Blockchain technology based solution that can mitigate myriads of threats against OSNs and thus provide OSNSDP. Other contributions made in the paper are: (i) the presentation of a taxonomy of Blockchain technology from the perspective of Context of Softwarization regarding the threats and how to manage them; (ii) sample scenarios of users (as victims) and attackers with a hybridization of possible attacks; and (iii) a fine-grain of activities that are needed to guide the correct identification of functional and nonfunctional requirements.

The authors maintain that the presentations in this paper provide significant insights to the domain of Internet technology, OSN, Blockchain Technology, and user requirements engineering generally while the framework with its methodological constituents constitutes a re-usable paradigm, which can be useful in the area of functional and nonfunctional requirements elicitation. The blockchain taxonomy that was presented with respect to OSNSDP is equally important. It provides useful insight to stimulate further research among those who are proponent of softwarization as the way to address online threats using the technology of Blockchain and its attendant consensus mechanism with inputs from the business modelling perspective. In future, to complement the contributions in this work, personas will be given attention since it supports softwarization in such a way that the designs created resonate with users' needs as a useful supplement to the use of scenarios. Though the contributions in this work is new, the contributed framework is prescriptively relevant since it is reproducible as affirmed by the requirements, taxonomy and personas that are presented. In the future, personas will be extensively considered along with appropriate theoretic models to analyse them with scenarios to further expand knowledge and understanding of specific protection mechanisms.

Acknowledgement

We acknowledge all members of the Information Storage and Retrieval Research team of the Department of Computer Science and engineering, Obafemi Awolowo University for their critique and suggestions that helped the research work to see the light of day.

Conflicts of interest

The authors of this research declare that they have no conflicts of interest.

Contribution of the authors

1. Conceptualization: Idepefo, F.O; Akhigbe, B.I; Afolabi, B.S.
2. Data curation: Idepefo, F.O; Akhigbe, B.I
3. Formal analysis: Idepefo, F.O; Akhigbe, B.I
4. Acquisition of funds: Idepefo, F.O; Akhigbe, B.I
5. Research: Idepefo, F.O; Akhigbe, B.I; Afolabi, B.S.
6. Methodology: Idepefo, F.O; Akhigbe, B.I; Afolabi, B.S.
7. Project administration:; Akhigbe, B.I; Afolabi, B.S.
8. Resources: Akhigbe, B.I
9. Software: Idepefo, F.O; Akhigbe, B.I
10. Supervision: Idepefo, F.O; Akhigbe, B.I
11. Validation: Idepefo, F.O; Akhigbe, B.I
12. Display: Idepefo, F.O; Afolabi, B.S.
13. Drafting - original draft: Idepefo, F.O; Akhigbe, B.I; Afolabi, B.S.
14. Drafting - revision and editing: Idepefo, F.O; Akhigbe, B.I; Afolabi, B.S.

Financing

This research has been funded by the authors of this research.

Referencias

Ahn, S., & Chong, K. (2006). Eliciting potential requirements with feature-oriented gap analysis. In International Conference on Software Reuse (pp. 427-431). Springer, Berlin, Heidelberg.

Aiello, L. M., & Ruffo, G. (2012). LotusNet: Tunable privacy for distributed online social network services. Computer Communications, 35(1), 75-88. Ali et al., 2014

Bahri, L., Carminati, B., and Ferrari, E. (2018). Decentralized privacy preserving services for online social networks. Online Social Networks and Media, 6, 18-25.

Beigi, G., & Liu, H. (2020). A Survey on Privacy in Social Media: Identification, Mitigation, and Applications. ACM Transactions on Data Science, 1(1), 1-38.

Bellini, E., Iraqi, Y., & Damiani, E. (2020). Blockchain-based distributed trust and reputation management systems: a survey. IEEE Access, 8, 21127-21151.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 36, 55-81.

Cox, K., Niazi, M., & Verner, J. (2009). Empirical study of Sommerville and Sawyer's requirements engineering practices. IET Software, 3(5), 339–355.

Curcio, K., Navarro, T., Malucelli, A., and Reinehr, S. (2018). Requirements engineering: A systematic mapping study in agile software development. Journal of Systems and Software, 139, 32-50.

Cutillo, L.A., Molva, R., and Strufe, T. (2009). Privacy preserving social networking through decentralization. In 2009 Sixth International Conference on Wireless On-Demand Network Systems and Services. IEEE, 2009, pp. 145–152.

De Salve, A., Mori, P., and Ricci, L. (2018). A survey on privacy in decentralized online social networks. Computer Science Review, 27, 154-176.

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy?. IEEE Cloud Computing, 5(1), 31-37.

Faily, S., & Fléchais, I. (2010). Security through usability: a user-centered approach for balanced security policy requirements. In Poster at: Computer Security Applications Conference - ACSAC '10. Annual, Dec., 2010 (pp. 1-2).

Fogues, R. L., Murukannaiah, P. K., Such, J. M., & Singh, M. P. (2017). Sharing policies in multiuser privacy scenarios: Incorporating context, preferences, and arguments in decision making. ACM Transactions on Computer-Human Interaction (TOCHI), 24(1), 1-29.

Garay, J., & Kiayias, A. (2020). SOK: A consensus taxonomy in the blockchain era. In Cryptographers' Track at the RSA Conference (pp. 284-318). Springer, Cham.

Garay, J., Kiayias, A., and Leonardos, N. (2015). The bitcoin backbone protocol: Analysis and applications. In Annual International Conference on the Theory and Applications of Cryptographic Techniques. (pp. 281 - 310). Springer.

Gervais, A., Karame, G.O., Wust, K., Glykantzis, V., Ritzdorf, H., and Capkun, S. (2016). On the security and performance of proof of work blockchain. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 3–16). ACM.

Ghosh, A., Gupta, S., Dua, A., & Kumar, N. (2020). Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. Journal of Network and Computer Applications, 102635.

Goguen J. A. (1993. Social issues in requirements engineering. In Proc. RE, pp. 194–195.

Goker, A., & Myrhaug, H. (2008). Evaluation of a mobile information system in context. Information processing & management, 44(1), 39-65.

Graffi, K., & Masinde, N. (2020). LibreSocial: A Peer-to-Peer Framework for Online Social Networks. arXiv preprint arXiv:2001.02962.

Guidi, B. (2020). When Blockchain meets Online Social Networks. Pervasive and Mobile Computing, 62, 101131.

Han, X., Martinez, V., & Neely, A. (2018). Service in the platform context: A review of the state of the art and future research. In Collaborative Value Co-creation in the Platform Economy (pp. 1-27). Springer, Singapore.

Helo, P., and Shamsuzzoha, A.H.M. (2020). Real-time supply chain: A blockchain architecture for project deliveries. Robotics and Computer Integrated Manufacturing, 63 (101909), 1-14.

Iannelli, L., Giglietto, F., Rossi, L., & Zurovac, E. (2020). Facebook digital traces for survey research: Assessing the efficiency and effectiveness of a Facebook Ad–based procedure for recruiting online survey respondents in niche and difficult-to-reach populations. Social Science Computer Review, 38(4), 462-476.

Iqbal, R., Sturm, J., Kulyk, O., Wang, J., & Terken, J. (2005). User-centred design and evaluation of ubiquitous services. In Proceedings of the 23rd annual international conference on Design of communication: documenting & designing for pervasive information (pp. 138-145).

Iqbal, J., Ahmad, R. B., Khan, M., Alyahya, S., Nizam Nasir, M. H., Akhunzada, A., & Shoaib, M. (2020). Requirements engineering issues causing software development outsourcing failure. PloS one, 15(4), e0229785.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011). Reverse social engineering attacks in online social networks. In International conference on detection of intrusions and malware, and vulnerability assessment (pp. 55-74). Springer, Berlin, Heidelberg.

Joshi, G. P., Perumal, E., Shankar, K., Tariq, U., Ahmad, T., & Ibrahim, A. (2020). Toward Blockchain-Enabled Privacy-Preserving Data Transmission in Cluster-Based Vehicular Networks. Electronics, 9(9), 1-15 (1358).

Koll et al., 2017), Koll, D., Schwarzmaier, M., Li, J., Li, X. Y., & Fu, X. (2017, June). Thank you for being a friend: An attacker view on online-social-network-based sybil defenses. In 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW) (pp. 157-162). IEEE.

Krcmar, H., & Hein, A. (2020). TP2.4: Business models of platform providers. http://tum-llcm.de/en/project/ap2/tp24/. Accessed 09/19/. Retrieved on 04-12-2020 @ 09:08 am.

Kumari, A., Gupta, R., Tanwar, S., & Kumar, N. (2020). A taxonomy of blockchain-enabled softwarization for secure UAV network. Computer Communications, 161, 304-323.

Kurtanović, Z., & Maalej, W. (2017). Mining user rationale from software reviews. In 2017 IEEE 25th International Requirements Engineering Conference (RE) (pp. 61-70). IEEE.

Liu, C., Zhu, T., Zhang, J., & Zhou, W. (2020). Privacy Intelligence: A Survey on Image Sharing on Online Social Networks. arXiv preprint arXiv:2008.12199.

Lo, S. K., Lu, Q., Wang, C., Paik, H., & Zhu, L. (2020). A systematic literature review on federated machine learning: From a software engineering perspective. arXiv preprint arXiv:2007.11354.

Lopez-Lorca, A. A., Miller, T., Pedell, S., Mendoza, A., Keirnan, A., & Sterling, L. (2014). One size doesn't fit all: diversifying" the user" using personas and emotional scenarios. In Proceedings of the 6th International Workshop on Social Software Engineering (pp. 25-32).

Mindila, A.N., Wafula, J.M., Ratemo, H. A., Tabu, C., Charo, J., & Silali, C. (2019). Requirements elicitation for a blockchain vaccine supply chain management web/mobile application. Gates Open Research, 3(1420), 1420.

Moeckel, C. (2018). Building Attacker Personas in Practice—a Digital Banking Example. In Proceedings of the 32nd International BCS Human Computer Interaction Conference 32 (pp. 1-5).