International Journal of Informatics and Computation (IJICOM)
Vol. 3, No.2, December 2021
ISSN: 2685-8711, E-ISSN: 2714-5263 DOI : 10.35842/ijicom

# Modern Privacy-Preserving and Security Schemes in Social Networks: A Review

Putra Wanda[1], Irma Permata Sari[2], Rizka Ayu Setyani[3], Niken Bayu Argaheni[4]

**Abstract The**
Online Social Network (OSN) is a popular application to exchange messages over the internet. However, millions of users are still under threat because of protection drawbacks. Many papers have proposed security methods, including firewalls, protocols, cryptography, statistical analysis, even learning algorithms. This paper provides an overview of privacy and security issues and describes multiple OSN protection techniques. We present various security schemes in OSNs and outline existing solutions to mitigate those attacks. This paper also discusses future research directions regarding OSN security problems and techniques.

**Keywords:**
Review, Modern Security Model, Online Social Network, Intelligence Schemes



## 1. Introduction

Mobile communication is an exploding technology evolution that increases the capacity and outperforms traditional cellular networks [1]. Many pieces of research have been done in the mobile network in various areas such as Wireless Sensor Network [81][82][83][84]. Online Social Network (OSN) is a widespread application in a mobile environment that enables users to exchange messages, pictures, videos, or even private information. Public OSNs, such as Facebook, Google+, and Twitter, become the most important platforms to build social connections. Nowadays, Facebook has 1.94 billion monthly users [45], while Twitter has over 313 million [46].

OSN providers can protect sensitive information against outside or even inside attacks. Thus the OSN users think the environment is secure and trustable in building digital interaction [2]. It makes most of the network users unaware of the critical threats in their environment. The unawareness enables unauthorized people to pose dangerous attacks [3]. Besides, the rapid growth of OSN users faces an increasing rate of attacks and data leakage. The environment remains a weakness in protecting private information from phishing or other threats in the OSN server. A weak system is the main reason for unauthorized entities to be able to compromise users' privacy. Intruders can pass the privacy-preserving strategy to compromise the users by using sophisticated algorithms to reveal the information. Thus, privacy-preserving is one of the most crucial and significant concerns on research issues.

User privacy issues in OSN usually come from outside attackers. However, when the provider policy remains uncertain when installing the application, it can be an inside issue if the users must sign a not understandable Term of Services (TOS) agreement that informs the application's privacy rule [6]. Not only long and challenging, but the

**Corresponding Author:**
1 Putra Wanda1, Universitas Respati Yogyakarta, Indonesia
2 Irma Permata Sari, Universitas Negeri Jakarta, Indonesia,
3 Rizka Ayu Aetyani, Universitas Sebelas Maret Surakarta, Indonesia,
4 Niken Bayu Argaheni, Universitas Sebelas Maret Surakarta Indonesia,

agreement is also further changeable and frequently incomplete. Surprisingly, the violation of the user terms of an OSN enables about 10% of all profiles (approximately 150 million accounts) to be Fake [7]. For server-side purposes, the large scale of OSN data in tremendous usages is one of the most valuable resources for OSN providers [8].

For a long time, cryptography is a standard security approach in computer applications. However, a dynamic environment with a large user and limited devices like smartphones makes it obsolete. The current issue is not just randomizing the plain text message (original) to become a chipper text (random message) but predicting and detecting malicious applications or activity in real-time. Moreover, conventional cryptography remains a drawback in computation overhead in the process. Costly computation and shortage of power cause the approach to become inefficient. Thus, mobile devices need an efficient algorithm to address the limitations of resources and deal with overhead computation [4]. Currently, several studies explore several methods by using verification messages, safe storage, and anonymity link among users to constitute the OSN protection [5].

Commonly, most of the security techniques utilize cryptosystems like RSA and Triple DES. It is a popular security method by randomizing the plain text message (original) to become a chipper text (random message) [15]. To enhance the OSN immunization, a community applies the protocol by proposing a mobile signature with Public Key Infrastructure (PKI) and the Session Initiation Protocol (SIP) [25] or integrating some protocols to establish multiprotocol like Pidgin AOL communicator to provide a common platform for the OSN [23]. The protocol can streamline cloud communications infrastructure and support for both IP and conventional communication lines. Another paper extracts user behavior data that adopt a trend screen brightness authentication, and it is called BrightPass [37]. A study can build a content experience for the prospect customer by analyzing the behavioral data and construct a security model with learning techniques by using CNN or Long Short-Term Memory (LSTM) to classify OSN account based on feature computation [61]. Other current research in OSN security approaches is using sophisticated learning techniques [85][86][87][94].

By reviewing essential papers and combined with the authors' experience in the field, we present the modern OSN security methods and a new direction for the next research in OSN security. The paper aims to identify the experiment gaps, highlight existing OSN security scheme limitations, and identify the privacy-preserving models' current methods. Our study hopefully becomes the gateway to establish the subsequent advances in OSN protection research. The primary contributions of this paper are as follows.

1. We present a review of the existing OSN security strategy. The paper introduces a precise definition of security and privacy in the OSN context. To construct an insightful and fruitful review paper, we gather many research papers in OSN protection, including publications and patents. We review various modern security schemes that cover OSN security schemes in public and private social networks.
2. This paper presents a broad scheme to address privacy leakage and introduce trust-based mechanisms to deal with the current privacy issue. This paper also presents a novel evaluation framework, especially in knowledge-based and trust-based schemes.
3. At the final stage, we outline open challenges and next research opportunities. Our review provides the research challenges, envision further study, opportunities, and outline the security schemes recommendations.

To achieve the best outcome for undertaking the study, we conduct literature reviews to make a well-defined methodology and hinder bias results. Firstly, we identify the literature review necessities, define the paper's research questions, and evaluate the

protocol for conducting the documents' review. We undergo the following step for doing the literature review: At the initial phase, we identify the research, choose literature, extract, and synthesize the data. Finally, we describe the research technique in more detail and conduct essential activities for this study

## 2. Background

1. Online Social Network

The typical OSN architecture is client-server and Peer-to-Peer (P2P). In client-server communication, all messages from the sender must pass through the server. Several papers propose the security model of client-server by using SIMPP (Secure Instant Messaging and Privacy Presence) [9] or a Jabber protocol [10]. In the paper, the model provides a local server to receive messages that have local storage to keep user data such as contact lists and preferences. However, when the client sends the messages to the local server or through many local servers, the security issues remain high because the drawbacks can increase tapping attacks' chances. In the broader scope of communication architecture, several papers propose efficient infrastructures [75] [76] [77] by constructing state-of-the-art methods [78] [79] [80].

To measure the OSN server protection level, a study investigates the protection model with the Wireshark packet sniffer and Forensics Tool Kit (FTK) [16]. It explores the security level provided by a public server, especially in encryption and sniffing techniques in the OSN. Although the OSN apps propose encryption data, multi-party control has become a challenging issue. To increase server protection in OSN, several methods can be applied, including the re-encryption model [17], public-key cryptography [18], and attribute-based encryption (ABE) technique [29].

Different from client-server, the P2P social network allows users to send messages directly without a third party. Some popular applications implement the model, including Telegram and WhatsApp [11]. A study proposes a P2P model with the virtual network to allow peers interaction and self-organize independently. It constructs several pipes as virtual channels for transmitting messages between services and applications that consist of searching and connecting the ends of a tube. The technique delivers data over the virtual channel with a specific algorithm [12]. A little bit different from the P2P model dubbed Pervasive Social Network (PSN), a two schemes model for securing communication by evaluating local trust in a distributed manner. By implementing attribute-based encryption, each node can control its data by trusting other nodes. [13]. Fig. 1. illustrates the PSN model with different nodes of communication.

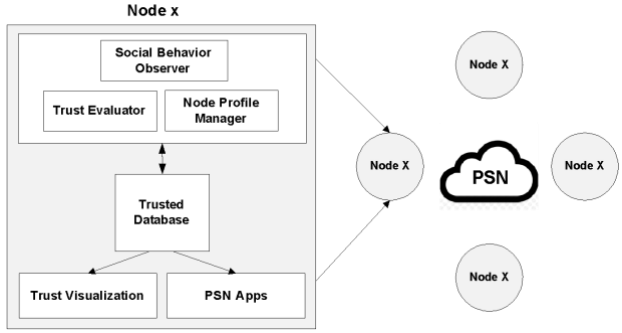


Fig. 1. A system model for securing Pervasive Social Network based on the trust in a distributed way

In the paper, the model utilizes algebraic operations using a Pairing-Based Cryptography (PBC) with a 160-bit elliptic curve group on the super singular curve x^3+x=y^2 over a base 512-bit finite field. It estimates the four primary operations in the schemes based on CP-ABE and KP-ABE, then implement the AES key with 128 bits in different LT levels in the testing processes. With the KP-ABE approach, LT levels can encrypt the key with the AES algorithm. However, the centralized PSN is so complicated and hard to implement in some specific situations (e.g., disaster regions, conflicts, and military activities). The remaining issues are how to automatically control the access when transmitting data over the public network against DDoS and internal attacks., a reliable and efficient way in PSN is a challenge.

## 2. Conventional OSN security schemes

A weak system enables attackers to spread malware, takedown system, install bots, or even damage machines. Some cases show the data leakage risks both on the private and the public OSN. For instance, in MSN's leakage case, we find various issues within the central processing device. Although MSN is better and with integrated controls to improve the system's level, it remains the big question of what and when the risks occurred in detail. A paper discusses a specific type of Sybil attack in MSN, focusing on the security mechanism to detect Sybil nodes and eliminate them. It is to ensure the routing while forwarding process. The model combines measuring distance in the client-side and removing process in the server-side, respectively [14].

Not just Sybil attacks from outside attackers, modern OSNs' with client-server model remain as issues for insider trust. The OSN provider should protect all personal and user identity in their system. However, service providers can benefit the user information for profit action, such as examining and sharing for advertising purposes. OSN server enforces clients to put private data and faith in it. The incapability to keep client information from suspicious activity causes leakage and revealing the data to the public. Current public OSN adopts several conventional techniques to achieve better OSN security by utilizing traditional algorithms, like RSA and Triple DES. The algorithms are widely becoming an agile approach to enhance immunization in the OSN [15].

Instead of using conventional cryptosystems such as RSA, Diffie-Hellman, or ElGamal, a paper explores an OSN security model by a Hash function(SHA) to validate user message when transmitting over the network. In the running process, the model determined an F(M) function, with M as the changeable message's length. However, if message M consists of M1 and M2, the first generated code can be detected easier. It is not sufficient for OSN with large spectrum users [21].

To increase the security with SHA, a technique combines the SHA with Off The Record (OTR) protocol. The method runs by combining cryptosystems in the environment and utilizing secure encryption with the AES symmetry algorithm, Diffie-Helman as the key, and SHA-1 as the Hash function. The OTR privately supports sending messages among users because the communication runs in a particular encrypted channel [22]. To increase the OTR protocol, another study explores OTR multiprotocol operation to enable the ability to connect with clients of various OSN connections. It has message encryption with a well-known AES 128 bit and key exchange process. The model integrates some protocols to achieve better level immunization. The study adopts multiprotocol like Pidgin AOL communicator to provide a common platform in each protocol so that the client can enjoy their protocol or identifier for peer's OSN [23].

To establish community transaction, another paper proposes security with a cryptosystem [24]. It builds trust for a centralized communication group and applies the ElGamal, RSA algorithm, and Chinese Remainder Theorem [19]. Another study explores a lightweight mobile signature with PKI and SIP to generate a digital signature to sign an electronic document [25]. However, it is challenging to implement in a mainstream OSN such as WhatsApp and WeChat.

To deal with the above problem, a paper explores the protection technique for Mobile OSN by combining cryptosystems [26]. The model provides the ECC and the AES algorithm to construct the OSN security and implements Diffie–Hellman (CDH) to carry out a key agreement between users and obtain the key's assumption by updating the ephemeral key periodically. Utilizing timestamps and the ECC algorithm can deal with the denial of attack and forgery attack by storing the ciphertext data to prevent privacy leakage. Fig. 2. depicts the mobile OSN model with a combination of ECC and AES.

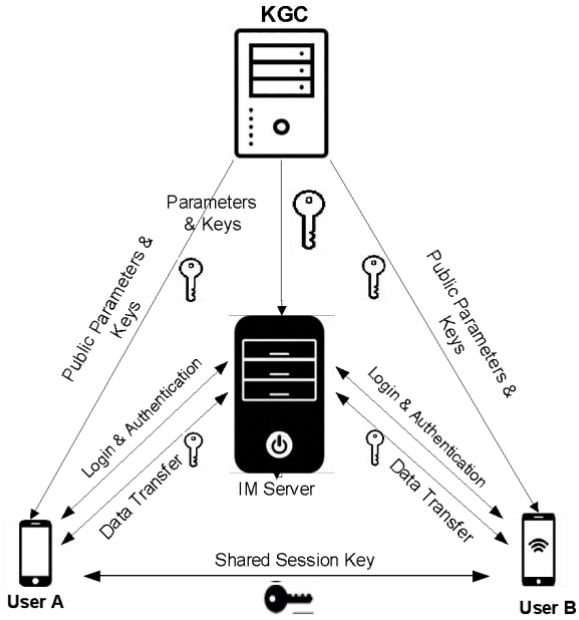


Fig. 2 Security model with ECC and AES combination.

It has three modules: Key Generation Center (KGC), IM server, and IM client. To ensure the security of the public-key cryptographic algorithm, the model builds the KGC part.

In the above architecture, KGC ensures the public-key cryptographic security, selects appropriate parameters, and publishes it into the OSN environment. With the user's unique identifier, the KGC generates a key pair (public/private key) and sends the private key to the user in a secure channel as a sharable session key. To gain adequate results in the computation process, they apply d(n) type elliptic curve group with 160-bit order in each communication session. Parameter d(n) denotes the field size of n bits. It is better for small group elements [27].

However, conventional ECC requires high computation, and it will be worse when computing the big size of the text. To address the issue, researchers should choose the value of the most suitable curve to achieve efficient computation, especially in mobile computation. In dynamic OSN, client-server architecture remains risky. It is challenging to provide efficient privacy-preserving with a large user. Besides, there are various AES attacks, such as side-channel attacks to reveal the AES key in hardware

and successful cache attack against AES-256 and AES-256-GCM via Graphical Processing Unit-based analysis [28].

In a dynamic environment like OSN, the conventional algorithm remains a drawback. For example, the RSA algorithm carries out the multiplication of two prime numbers, but factorization is a severe threat against RSA. There are many inefficient algorithms available that correctly factor big numbers. A study reveals severe security weaknesses in RSA. The research shows that it is possible to decrypt a ciphertext in the RSA by different secret keys [20].

Moreover, conventional approaches, including RSA, DES, ECC, Diffie-Helman, only curb the direct disclosure of personal information. They remain as shortcomings when the intruders intelligently combine large-scale unrelated information to hinder privacy's indirect exposure. Hence, the next phase of securing OSN is adopting suitable intelligence algorithms to gain a high level and real-time security.

The primary source of anomalous activities is the virus, malware, worm, or bots. During the software's design and implementation process, the root of the worm is the inevitable vulnerability. Thus, it is hard to avoid worms in the existing software engineering systems entirely because worms can pass through the resistant layer of the OSN nodes. To solve the hole, the administrator usually provides a patch to the system. However, due to a lot of bandwidth consumption, he cannot transmit the patch simultaneously to all network users. A study proposes a two-phase immunization strategy with network vertex influence. The model selects the most critical vertices in the entire connection. Minimum Dominate Set is an effective way to choose key nodes in the analysis process by considering the global condition. To obtain the best result of worm detection, the method enhances the selected vertices' security level [32].

Suspicious activities run unauthorized access without the user's consent to steal sensitive credentials like password, PIN, or even full identity theft. Just as a reminder, a popular OSN (Facebook) said, about 87 Million users might have been shared in the leak [33]. In worm issues, activities like reconnaissance or detecting reconnaissance activity are arduous. Reconnaissance is the initial process in the APT threat [34]. A paper introduces a framework for OSN honeypots management to enhance the detection of Advanced Persistent Threats (APTs) at the reconnaissance phase. The model can obtain warnings of further attacks and simulate integrated fake profiles that enable us to generate both manual and automatic honeypot [35]. Another paper also researches classifying user behavior in a large OSN dataset, Tencent QQ. It adopted the normalized Random Forest (RF) as the statistical classifier and evaluated its detection rate accuracy [31].

Malicious activities also become a concern in OSN implementation for financial transactions. ProGuard is a model to detect malicious accounts in OSN within online promotion activities. It enables us to identify suspicious participants in promotion events, especially in virtual currency collection and integrates features systematically to characterize accounts from three perspectives, including behaviors, recharging patterns, and currency usage [30]. The model tries to address the integration problem between OSN and financial accounts. Fig. 3. depicts an OSN model with ProGuard architecture.

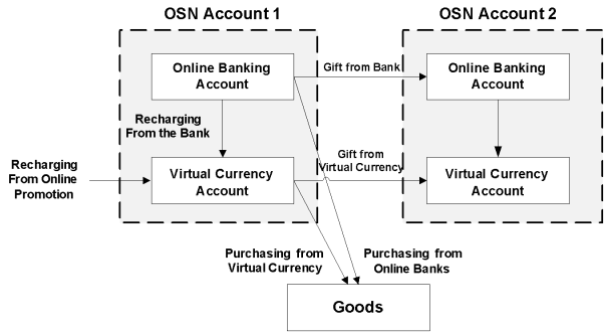


Fig. 3. ProGuard model to integrates OSN and financial accounts. Within the ProGuard user, it has Online Banking Account and Virtual Currency Account.

## 3. Privacy-Preserving Schemes in Social Network

To gain privacy in OSN, the community should concern about a vital element, including policy aggregation and user relationship. A paper explores an effective policy aggregation method to enable or disable resource sharing based on all users' authorization conditions. To measure the privacy risk, it applies a logical representation and develops a feature like Facebook Canvas to demonstrate the access control model's feasibility [41]. However, the technique remains a shortcoming when merging many privacy settings. It is a complicated process because policies may conflict. That could remain as user difficulty if they are unable to control shareable information on the network.

Sharing information requires a trust management system network, especially in Pervasive OSN (POSNs). It needs a framework to generate high trust value between the users with a lower cost of monitoring. It constructs a Flexible Mixture Model (FMM) to quantify the system around six different properties and apply Osmotic Computing to undergo computational offloading. It reduces the excessive utilization of resources over an individual server. As a result, it harvests the prediction rate in the range of ±2% (low errors rank) [42].

The privacy-preserving scheme can also collaborate [40] [43]. For example, a paper proposes a bandit mechanism to solve the privacy issue. According to an aggregated opinion, a user decides whether or not to post a data item. The method needs to gather the stakeholders' views and get a decision rate to calculate the trust-weighted voting scheme. If the owner has tagged all the stakeholders in d, the service provider can act as an agent to notify the stakeholders. Fig. 4. illustrates trust-based privacy management.

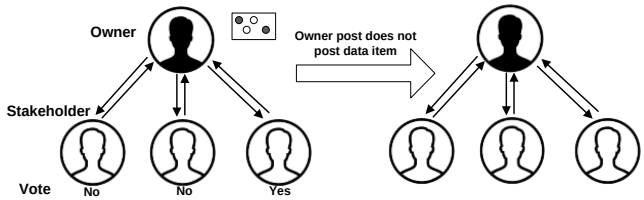


Fig. 4. The illustration depicts that the owner's trust in the stakeholder is represented as the thickness of the blue line.

The stakeholder's trust in the owner denotes the thickness of the green line. The stakeholder's trust in the owner updates the value after the owner gains the data posting decision. The level of the owner's trust determines whether to approve or disapprove of the data posting.

The study employs a bandit approach to tune the threshold in the trust model. The user gets a high long-turn payoff as the difference between the benefit of posting data and user privacy loss. In the bandit problem, the participant's reputation is influenced by their historical interactions with other users; hence, user activity has determined the rewards of arms. The bandit model was similar to another bandit problem approach [44]. Nevertheless, a model implements a weak regret concept for adversarial bandit problems to measure the model's performance. The weak regret formulation is calculated by:

$$R_{weak}(T) = max_{i=1,..,K} \sum_{t=1}^{T} r_{i,t} - \sum_{t=1}^{T} r_{I,t} \quad (1)$$

Calculation performance of the weak regret results in a learning policy. It is compared with a hypothetical benchmark policy that always chooses the best. The benchmark policy with the best arm is not the one that corresponds to the maximally expected reward. Based on our modern protection review, the privacy-preserving model with collaborative management can be a practical solution to the OSN. It can resolve privacy conflict for collaborative data sharing and address the multi-party adaptive computational mechanism's multi-party problem [39]. Moreover, a practical and real-time security model with automatic feature engineering can be a promising solution in the OSN dynamic environment. Table 1 describes various protection models that show the state of the art.

## 4. Current Security Approach

Instead of using cryptosystem, statistic, or manual rule-based, the current OSN system should construct intelligence and a real-time security model. It needs to build a learning model because the OSN environment contains vast and dynamic data [45], so it needs a sophisticated model to deal with various environmental threats. Thus, artificial intelligence is a current and practical solution to elevate security model capabilities.

1. Bringing Deep Learning as OSN intelligence security

   The modern security model in OSN is becoming the primary concern in the dynamic interaction system. The current paper analyzes OSN activity patterns using a machine learning algorithm in nearly 9,000 Facebook wall messages as the dataset. The paper finds the content-type is not the essential feature, but demographics such as gender and age are informative predictors [38].

   Another paper proposed a standard learning algorithm, Naïve Bayes, to deal with classification problems in spam detection. A paper undergoes anomalous text analysis to classify spam in network communication. The study constructs spam detection using the Naïve Bayes algorithm for multi-classification and multi-two classifications. They conduct text preprocessing by calculating regular expression and computing feature extraction with TF-IDF (Term Frequency-Inverse Document Frequency) algorithm [53]. However, it remains a drawback when the naïve Bayes classifier only relies on an often-faculty assumption of equally essential and independent features, resulting in biased posterior probabilities.

Recent studies revealed that cybercriminals tend to exchange knowledge about cyber-attacks in OSN. It requires constructing a modern security model to detect cybersecurity-related accounts on OSN and monitor their activities automatically. A paper proposed automatic detection of cybersecurity-related accounts on Twitter to discover unknown cybersecurity experts and cybercriminals for monitoring purposes. The paper presented three machine learning including decision trees, RF, and SVM to deal with the classification. Experimental results showed that both decision trees and RF had performed well with an overall accuracy of over 95%, and RF accuracy had reached as high as 97.877% [89]. However, conventional machine learning suffers from manual feature engineering in massive datasets like OSN. Thus, research and implementation costs using this manual model become bigger.

In the current years, deep learning is being exploited to analyze and detect OSN threats, such as labeled and unlabeled applications, by training various deep learning architecture models. Neural networks can extract features from OSN node behaviors and activities as the important features to construct an effective security model in the OSN [88]. For example, a paper proposed an efficient RNN to detect malware using different values of hyperparameters [91].

Sentiment analysis is an essential element in OSN analysis that consists of a word or sentence level analysis. Another open question in the sentiment analysis issue is how to detect tension in online communities. A paper proposes detecting the tension model in OSN. It explores the spikes feature in OSN tension by measuring the level of deterioration in the relationship between individuals or groups [52]. To elaborate the analysis for textual prediction, it can be developed using Weakly Supervised Multimodal [74]. Dataset of sentiment analysis research can be obtained from SemEval [48] or Amazon corpus [49].

In the sentiment training process, a study requires the Tweet2Vec to learn embedding has labeled English tweets data using character-level CNN and LSTM [50]. It computes the similarity of semantic and sentiment categorization in a tweet. The model calculates the sequence of character and word n-grams of CNN. However, those approaches fail to solve several significant OSN analysis challenges, such as abbreviations, special characters, and informal languages, spelling errors. Thus, it requires a string transformation method, such as Word2Vec [51].

Not just analyze malicious sentiment by using learning technique, another issue is how to detect malicious activities or spam by using deep learning [60] [62]. Malicious detection is a kind of a practical method to build security policies. The current study proposes malicious account detection by adopting the long short-term memory (LSTM) in the Momo OSN dataset [61]. To build detection model, a study can harness the behavior dataset [36] [63] [70]. For example, COMPA establishes a technique to detect compromised accounts and anomaly detection by analyzing behavioral data. Using two parameters: content similarity and URL similarity, the technique can divide similar content and compromised accounts [63]. Another promising approach is BrightPass, a framework with a user behavior analysis that adopts a trend screen brightness authentication [37].

Tobiyama et al. [88] proposed malware detection based on behavior. The study implemented LSTM for feature extraction and CNN for classification to train process behavior in a sequence of API calls. The features were extracted from the process behavior log files will be transferred to an image that contains local features. These local features represent the process activities to enable people to apply CNN to capture these local features and correctly classify these images. Fig.5 illustrates the Deep Learning model as the OSN security model.

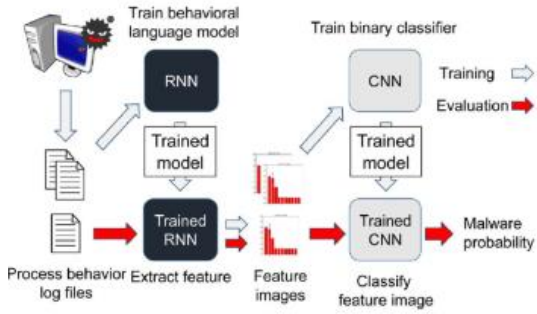


Fig. 5. The illustration of Deep Learning architecture as the security schemes in OSN. It can be a new solution to detect malicious activities in dynamic environments.

OSN has a million connections among the user, so a link prediction may become a new method to analyze suspicious activities and to detect current threats such as Sybil. The sophisticated Sybil attack undergoes the threat to collapse and subverts the reputation system by creating multiple pseudonymous accounts. They try many techniques to collapse the reputation system, including spreading spam, leveraging Sybil friendship to de-anonymize the OSN environment, and impersonating another account. An infected account may generate many Sybil accounts and harness them to conduct unauthorized action, including sending botnet or making fake vote ranking. If a system utilizes CAPTCHA as the security model against an automated Sybil attack, it remains risky and breakable [64]. Fig. 6. depicts the Sybil accounts attacks connection when infecting the OSN system.

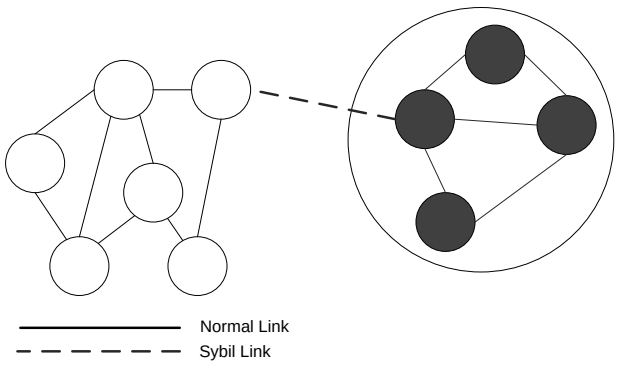


Fig. 6. Sybil accounts attack connection model in an OSN environment. Sybil protections are a very critical part of maintaining the proper operation in a system.

To address the Sybil problem in link prediction, analyzing link anomaly is widely used as a security parameter by extracting anonymous social graph using Sequentially Discounting Normalized Maximum Likelihood (SDNML) [65], seed information [66], and knowledge graph [67] or weak estimators [68]. To elaborate learning algorithm in link prediction, current papers introduce Restricted Boltzmann Machine (RBM) [69] or Deep Belief Network [58]. The further technique to deal with Sybil should support link predictions

because the conventional statistical method cannot detect anomalies like zero-day attacks or unexploited vulnerabilities.

In current years, Facebook adopts AI to detect suicidal thoughts, LinkedIn predicts the highest match for the users' role, and Twitter is using a neural system to crops a picture using face detection [47]. Current studies present ML algorithms to classify various information, such as age [54], location [55], language [56], and political preference [57], link prediction [58], even crisis response [59].

Besides, toxic activities like cyberbullying are disturbing online misbehavior with troubling consequences. The issue appears in different forms in most of the social networks in textual format. Automatic detection of such incidents requires intelligent systems. Existing cyberbullying detection studies applied conventional machine learning that just can adaptable to a single OSN at a time. In current years, deep learning techniques find their way in detecting cyberbullying incidents to deal with conventional learning limitations and improve the detection performance. It can also benefit from integrating other sources of information and looking into the impact of profile information of the OSN users [90].

2. Blockchain as new OSN security approaches

The client-server model suffers from personal data leakage, protection drawbacks, and ownership of information. In the future, the client-server OSN with centralized control may disappear with Blockchain technology as a breakthrough to construct the next-generation OSN decentralized models. Principally, the method is better to control the contents because they keep their data in all services. By diminishing the central unit, no entity can monitor and control the user content and personal information.

In operation, the Blockchain acts as a ledger to record all transactions and share them with the network participants [71]. To construct OSN protection, a study presents a technique to build decentralizing privacy using Blockchain. In the model, the Blockchain accepts two types of transactions consisting of $T_{access}$, for access control management, and $T_{data}$ for data storage and retrieval. The model has three elements: the system entity for downloading the application, services for running processing personal data, and user entities to maintain the Blockchain. Both the service and the user can obtain the data $T_{data}$ transaction by using their key. The blockchain model will verify whether the digital signature belongs to the user or the service [72]. Fig.7 illustrates the decentralized model of OSN security with Blockchain.

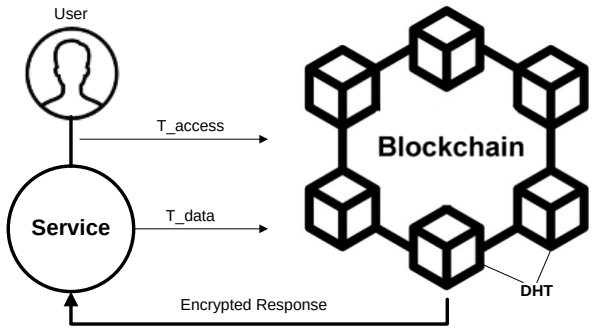


Fig. 7. The decentralized platform of OSN with Blockchain.

In OSN protection, the Blockchain can also be applied for establishing a trustworthy environment to create value for user-generated content. A study proposes BEV-SNS, a framework for incentivizing user behavior on OSN. The model has a goal to gain control over data access and build value creation via OSN transactions. It contains an inherent architecture of blockchains to enable the user to tune the sharing parameters and rewards in BEV-SNS. It can predict the many accounts creation and give prorate rewards for SNS-specific behavior based on the bots' content [73].

Adding blockchain technologies to construct P2P secure connections in OSN becomes promising as the modern OSN system is pruning to P2P architecture [11]. P2P social networks promise to support end-to-end communication, strict access control, anonymity and resilience against censorship, and massive data leaks through misused trust. Thus, blockchain technology becomes a promising solution as the new way of OSN protection [92].

Table 1. Multiple techniques to establish the OSN protection model.

| Objective | Method |
|---|---|
| To avoid overhead computation in securing process of OSN | Group Authentication [4] |
| Design of instant messaging using identity-based cryptosystems | Elliptic Curve Cryptography (ECC) [9] |
| Defending Sybil attacks in mobile social networks | Distance algorithm in client-side [14] |
| To build a digital signature for signing an electronic document | PKI and SIP [25] |
| Improving security and efficiency for encrypted data sharing | Partial decryption schema [17] |
| To detects anomalous activities in online social networks | User behavior analysis [62] |
| To detects worm activities with OSN. | Network vertex influence [32] |
| To build link prediction in signed social networks | Deep Belief Network (DBN) [58] |
| To builds an encryption mechanism for instant messaging in mobile devices. | ElGamal, RSA, and (CRT) [15] |
| Resolving multi-party privacy conflicts in social media | Adaptive computational [39] |
| To builds secure social communications based on trust in a distributed way | AES algorithm, CP-ABE, and KP-ABE architecture [13] |
| To integrates multiprotocol instant messenger securely. | OTR protocol and AES [ 23] |
| To detects malicious accounts in the social network in online promotion activities. | Normalized Random Forest (RF) [30] |
| To create OSN management for honeypots for detecting targeted cyber-attacks, | Designed APT framework [35] |
| To computes offloading value for manage trust in the OSN | Osmotic Computing [42] |

| | |
|---|---|
| To build multi-party access control in online social networks | Personally Identifiable Information (PII) [40] |
| To builds a trust-based collaborative access control model for online social networks. | Policy aggregation [41] |
| To measure dynamic privacy in multi-armed with time-variant rewards. | Bandit approach [44] |
| To detects compromised accounts on Twitter | User behavioral profile analysis [63] |
| To improve security in Mobile Social Network Access. Avoiding side-channel attacks in OSN | Screen brightness authentication [37] |
| To enhance privacy protection in social networks | Evolutionary game theory [36] |
| To enhanced message security and privacy protection scheme for mobile social network systems | ECC and AES algorithm [26] |
| To detects malicious account detection in the Momo OSN | The deep learning, Long Short-Term Memory (LSTM) [60] |
| For spam detection in mobile social networks | DL Multistage and elastic framework [61] |
| For predicting Microblog sentiments | Weakly Supervised Multimodal and CNN [74] |
| To build trust-based collaborative privacy management in OSN | Multi-armed bandit mechanism [43] |
| To protect personal data in building decentralizing privacy | Blockchain approach [72] |
| To enhance privacy protection of OSN framework | Designed Blockchain [73] |

# 5. Summary

Nowadays, most OSN architectures are client-server architecture, which is centralized control by the provider/server. This architecture relies on the servers as the center of communication and management, but it remains an issue in provider trust. Different from server-based OSN, a P2P architecture prioritizes direct communication among peers directly without the server role. We have revealed several security approaches based on these architectures.

On the other hand, various research communities construct a protection model by utilizing the cryptography approach. To improve the OSN security, many studies have introduced conventional techniques, including the DES, RSA, Triple DES, ECC, SHA, designed security protocol until the statistical analysis. However, these standard methods remain as drawbacks when the intruders intelligently combine large-scale unrelated information to hinder the indirect disclosure of privacy. Moreover, the conventional algorithms require a massive computing resource and are challenging to implement in limited hardware with different software, operating systems, and network domains. Hence, intelligence security schemes with automatic representation in OSN are becoming promising and an active research topic as modern techniques.

Based on our review, the following active area of OSN protection strategy uses a learning approach to analyze real-time behavior data, trajectories, and network information. How to implement an effective intelligence algorithm becomes the next phase of the adaptive protection model in OSN. Another ongoing trend is the arising of blockchain technology as the substitution of the centralized client-server OSN. It is a breakthrough technology that can construct the next-generation OSN decentralized models. By applying Blockchain, OSN can build a decentralized environment that increases data privilege and allows users to keep their data.

## Acknowledgment

This paper is conducted as a collaboration program between university researchers in Indonesia.

## References

[1]. Nait Hamoud, T. Kenaza, and Y. Challal. Security in device to device communications: a survey,. in IET Networks, 2017.
[2]. L.Cutillo, R.Molva, T.Strufe, Safebook: a privacy-preserving online social network leveraging on real-lifetrust,. IEEE Commun. Mag.47(12) 94–101, 2009.
[3]. G. Nalini Priya and M. Asswini. A survey on vulnerable attacks in online social networks,. International Conference on Innovation Information in Computing Technologies, Chennai, pp. 1-6.2015.
[4]. L. Ham. Group Authentication, IEEE Trans. Vehicular Technology;62(9), 2013.
[5]. S. Muftic, N. bin Abdullah, and I. Kounelis. Business information exchange system with security, privacy, and anonymity," J. Electr. Comput. Eng., vol. 2016, Art. no. 7093642, 2016
[6]. C. Fiesler, A. Bruckman, Copyright terms in online creative communities, in Proceedings of the Annual Conference Extended Abstracts on Human Factors in Computing Systems, CHI'14, ACM, pp.2551–2556. 2014.
[7]. I. Ahmad. (2015). How Many Internet and #SocialMedia Users are Fake? Retrieved : Apr. 2, 2015..: http://www.digitalinformationworld.com/2015/04/infographic-how-many-internetsusers-are-fake.html.
[8]. P. Gadkari. (2013). How does twitter make money?. Retrieved: Nov. 2013. Available: http://www.bbc.com/news/business-24397472
[9]. C.-J. Wang, W.-L. Lin, and H.-T. Lin. Design of an instant messaging system using identity-based cryptosystems,. pp. 277–281. 2013.
[10]. M. Serik and G. B. Balgozhina. Instant messaging application for smartphone,. Life Sci. J., vol. 11, no. SPEC.ISS.1, pp. 258–262. 2014.
[11]. B. Yuan, L. Liu, and N. Antonopoulos. A Self-Organized Architecture for Efficient Service Discovery in Future Peer-to-Peer Online Social Networks,. 2016 IEEE Symposium on Service-Oriented System Engineering (SOSE), Oxford, pp. 415-422. 2016.
[12]. P. Wanda, Selo and B. S. Hantono. ``Model of secure P2P mobile instant messaging based on virtual network,'' in Proc. Int. Conf. Inf. Technol. Syst. Innov. Bandung, Indonesia, pp. 8185, 2015.
[13]. C. Huang, Z. Yan, N. Li, and M. Wang. Secure Pervasive Social Communications Based on Trust in a Distributed Way,. in IEEE Access, vol. 4, pp. 9225-9238. 2016
[14]. Y. Sun, L. Yin and W. Liu. Defending Sybil attacks in mobile social networks,. 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, pp. 163-164. 2014.
[15]. Wenping Guo, Zhenlong L, Ying C, Xiaoming Z. Security Design for Instant Messaging System Based on RSA and Triple DES,. IEEE *2009 International Conference on Image Analysis and Signal Processing*, Taizhou, 2009, pp. 415-418. 2009.
[16]. N. B. Al Barghuthi & H. Said. Social networks IM forensics: Encryption analysis,. J. Commun., vol. 8, no. 11, pp. 708–715. 2013.
[17]. H. Qinlong, M. Zhaofeng, Y. Yixian, N. Xinxin and F. Jingyi. Improving security and efficiency for encrypted data sharing in online social networks,. in *China Communications*, vol. 11, no. 3, pp. 104-117, 2014.
[18]. A. Tootoonchian, Stefan S., Yashar G.,Alec W. Lockr: Better Privacy for Social Networks., Proc. 5th Ini'l Conf. Emerging Networking Experiments and Technologies (CoNEXT 09), pp. 169-180, 2009.
[19]. I. Del Pozo and M. Iturralde. CI: A new encryption mechanism for instant messaging in mobile devices,Procedia Comput. Sci., vol. 63, pp. 533538. 2015.
[20]. Majid B. Mohd A. Serious Security Weakness in RSA Cryptosystem. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3. 2012.

[21]. Yusof, M.K., & Abidin, A.F. A secure private instant messenger. *The 17th Asia Pacific Conference on Communications*, 821-825. 2011.
[22]. A. Nalawade, D. Kamdar, P. Angolkar, and S. Gaikwad. Integrated Instant Messaging System,. IJLTET. J., vol. 3, ISSN: 2278-621X, 2014. 2017.
[23]. S. Bala and T. Wasilczyk. Secure integration of multiprotocol instant messenger,. 2017 IEEE International Conference on Innovations in Intelligent Systems and Applications (INISTA), Gdynia, pp. 495-500. 2017.
[24]. M. H. Eldefrawy, K. Alghathbar, M. K. Khan, and H. Elkamchouchi. Secure instant messaging protocol for centralized communication group," in Proc. 4th IFIP Int. Conf. New Technol., Mobility Secur., Paris, France, pp. 1 4. 2011.
[25]. A. Ruiz-Martínez and C. Inmaculada Marín-Lòpez. ``SIPmsign: A lightweight mobile signature service based on the Session Initiation Protocol,'' Softw. Pract. Exper., vol. 44, no. 5, pp. 511 535, 2014.
[26]. Z. Wang, Z. Ma, S. Luo and H. Gao. Enhanced Instant Message Security and Privacy Protection Scheme for Mobile Social Network Systems,. in *IEEE Access*, vol. 6, pp. 13706-13715. 2018.
[27]. B. Lynn. The Pairing-Based Cryptography Library, 2013. Retrieved: http://crypto.stanford.edu/pbc/
[28]. B. Lapid & A. Wool. (2018). Cache-Attacks on the ARM TrustZone implementations of AES-256 and AES-256-GCM via GPU-based analysis,., https://eprint.iacr.org/2018/621.pdf
[29]. R. Baden, A. Bender, N. Spring, B. Bhattacharjee, D. Starin.. Persona: An Online Social Network with User-Defined Privacy., Proc. ACM SIGCOMM Conf. Data Comm. (SIGCOMM 09), 2009, pp. 135-146.
[30]. Y. Zhou *et al*.. ProGuard: Detecting Malicious Accounts in Social-Network-Based Online Promotions, in *IEEE Access*, vol. 5, pp. 1990-1999. 2017.
[31]. L. Breiman. Random forests, Mach. Learn., vol. 45, no. 1, pp. 5–32. 2001.
[32]. W. Yang, H. Wang, and Y. Yao.. An immunization strategy for social network worms based on network vertex influence, in China Communications, vol. 12, no. 7, pp. 154-166. 2015.
[33]. Forbes, 2018. Facebook Says Data On 87 Million People May Have Been Shared In Cambridge Analytica Leak, Retrieved: April 04, 2018. https://www.forbes.com/sites/kathleenchaykowski/2018/04/04/facebook-says-data-on-87-million-people-may-have-been-shared-in-cambridge-analytica-leak/#484f39eb3e8b
[34]. M. Ask, P. Bondarenko, J. E. Rekdal, A. Nordbø, Ruthven, and P. B Nordbo. (2013). Advanced persistent threat (APT) beyond the hype,. Presented at the IMT4582 Netw. Secur. GjoviN Univ. College
[35]. A. Paradise et al.. Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks,. in IEEE Transactions on Computational Social Systems, vol. 4, no. 3, pp. 65-79. 2017.
[36]. J. Du, C. Jiang, K. Chen, Y. Ren and H. V. Poor. Community-Structured Evolutionary Game for Privacy Protection in Social Networks,. in IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 574-589. 2018
[37]. M. Guerar, M. Migliardi, A. Merlo, M. Benmohammed, F. Palmieri and A. Castiglione. Using Screen Brightness to Improve Security in Mobile Social Network Access,. in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 621-632. 2018.
[38]. C. Fiesler et al. What (or who) is public?: Privacy settings and social media content sharing., Proc. ACM Conf. Comput. Supported Cooper. Work Soc. Comput., 2017, pp. 567-580.
[39]. J. M. Such, N. Criado. Resolving multi-party privacy conflicts in social media., IEEE Trans. Knowl. Data Eng., vol. 28, no. 7, pp. 1851-1863. 2016.
[40]. N. Vishwamitra, Y. Li, K. Wang, H. Hu, K. Caine, and G.-J. Ahn. Towards pii-based multi-party access control for in online social networks,. in Proc. 22nd ACM Symp. Access Control Models Technol., pp. 155–166. 2017.
[41]. N. C. Rathore and S. Tripathy. A trust-based collaborative access control model with policy aggregation for online social networks,.Soc. Netw. Anal. Mining, vol. 7, no. 1, p. 7. 2017.
[42]. V. Sharma, I. You, R. Kumar, and P. Kim.. Computational Offloading for Efficient Trust Management in Pervasive Online Social Networks Using Osmotic Computing, in IEEE Access, vol. 5, pp. 5084-5103. 2017.
[43]. L. Xu, C. Jiang, N. He, Z. Han and A. Benslimane. Trust-Based Collaborative Privacy Management in Online Social Networks,. in IEEE Transactions on Information Forensics and Security, vol. 14, no. 1, pp. 48-60. 2019.

[44]. L. Xu, C. Jiang, Y. Qian, Y. Zhao, J. Li, Y. Ren. Dynamic privacy pricing: A multi-armed bandit approach with time-variant rewards., IEEE Trans. Inf. Forensics Security, vol. 12, no. 2, pp. 271-285. 2017.
[45]. Zephoria, . The Top 20 Valuable Facebook Statistics, Retrieved: November 2017. https://zephoria.com/top-15-valuable-facebook-statistics/.
[46]. Twitter, Twitter Usage/Company Facts, Retrieved: November, 2017.
[47]. https://about.twitter.com/company.
[48]. Albert Smith. 2018, Why the Future of Social Media Will Depend on Artificial Intelligence., Retrieved: April 13, 2018, https://www.smartdatacollective.com/future-social-media-depend-artificial-intelligence/
[49]. Preslav Nakov, Alan Ritter, Sara Rosenthal, Fabrizio Sebastiani, and Veselin Stoyanov. (2016). SemEval-2016 task 4: Sentiment analysis in Twitter. InThe 10th International Workshop on Semantic Evaluation. Association for Computer Linguistics, 1–18.
[50]. Xiang Zhang, Junbo Zhao, and Yann LeCun (2015). Character-level convolutional networks for text classification. In Advances in Neural Information Processing Systems. 649–657.
[51]. Soroush Vosoughi, Prashanth Vijayaraghavan, and Deb Roy. Tweet2Vec: learning Tweet embeddings using character-level CNN-LSTM encoder-decoder. InThe 39th International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM, 1041–1044. 2016.
[52]. T. Mikolov, K. Chen, G. Corrado, J. Dean. Efficient Estimation of Word Representations in Vector Space., *Proc. Workshop at ICLR*. 2013.
[53]. P. Burnap, O. F. Rana, N. Avis, M. Williams, W. Housley, A. Edwards, J. Morgan, and L. Sloan.. Detecting tension in online communities with computational twitter analysis. Technological Forecasting and Social Change, 95:96–108, 2015.
[54]. Bin Ning, Wu Junwei, Hu Feng.. Spam Message Classification Based on the Naive Bayes Classification Algorithm.. IAENG International Journal of Computer Science, 46:1, pp46-53. 2019.
[55]. J. Zhang, X. Hu, Y. Zhang, and H. Liu.. Your age is no secret: Inferring microbloggers' ages via content and interaction analysis,. in ICWSM, Cologne, Germany. 2016
[56]. J. Zhang, J. Sun, R. Zhang, and Y. Zhang.. Your actions tell where you are: Uncovering twitter users in a metropolitan area,. in IEEE CNS, Florence, Italy. 2015
[57]. D. Nguyen, R. Gravel, D. Trieschnigg, and T. Meder. . how old do you think i am?; a study of anguage and age in twitter,. in ICWSM, Boston, IL, Jul. 2013.
[58]. X. Chen, Y. Wang, E. Agichtein, and F. Wang.. A comparative study of demographic attribute inference in twitter,. in ICWSM, Oxford, England, May. 2015.
[59]. Feng Liu, Bingquan Liu, Chengjie Sun, Ming Liu, and Xiaolong Wang.. Deep belief network-based approaches for link prediction in signed social networks. Entropy17, 4:2140–2169. 2015.
[60]. Dat Tien Nguyen, Shafiq R. Joty, Muhammad Imran, Hassan Sajjad, and Prasenjit Mitra. (2016). Applications of online deep learning for crisis response using social media information. CoRRabs/1610.01030. Retrieved from http://arxiv.org/abs/HYPERLINK
[61]. J. Wang, X. He, Q. Gong, Y. Chen, T. Wang and X. Wang. (2018). Deep Learning-Based Malicious Account Detection in the Momo Social Network,. 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, pp. 1-2
[62]. B. Feng, Q. Fu, M. Dong, D. Guo and Q. Li. (2018). Multistage and Elastic Spam Detection in Mobile Social Networks through Deep Learning,. in IEEE Network, vol. 32, no. 4, pp. 15-21, July/August.
[63]. B. Viswanath, M.A. Bashir, M. Crovella, S. Guha, K.P. Gummadi, B.Krishnamurthy, A.Mislove.. Towards detecting anomalous user behavior in online social networks, in Proceedings of the Twenty-Third USENIX Security Symposium, 2014.
[64]. M. Egele, G. Stringhini, C. Kruegel, and G. Vigna.. Towards detecting compromised accounts on social networks. IEEE Transactions on Dependable and Secure Computing, 14(4):447–460. 2017.
[65]. Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda. . All your contacts are belong to us: automated identity theft attacks on social networks. In Proceedings of the 18th international conference on World wide web, WWW '09, pages 551{560, New York, NY, USA. ACM. 2009.

[66]. T. Takahashi, R. Tomioka, and K. Yamanishi.. Discovering emerging topics in social streams via link anomaly detection. IEEE Transactions on Knowledge and Data Engineering, 26(1):120–130. 2014.
[67]. S. Ji, W. Li, N. Z. Gong, P. Mittal, and R. Beyah.. On your social network de-anonymizablity: Quantification and large-scale evaluation with seed knowledge.. in NDSS, San Diago, CA. 2015.
[68]. J. Qian, X. Y. Li, C. Zhang, and L. Chen.. De-anonymizing social networks and inferring private attributes using knowledge graphs,. in INFOCOM. 2016.
[69]. C. Chiu and J. Zhan. Deep Learning for Link Prediction in Dynamic Networks Using Weak Estimators,. in IEEE Access, vol. 6, pp. 35937-35945, 2018.
[70]. T. Li, B. Wang, Y. Jiang, Y. Zhang and Y. Yan. Restricted Boltzmann Machine-Based Approaches for Link Prediction in Dynamic Networks,. in IEEE Access, vol. 6, pp. 29940-29951. 2018.
[71]. Q. Gong et al.. DeepScan: Exploiting Deep Learning for Malicious Account Detection in Location-Based Social Networks,. in IEEE Communications Magazine, vol. 56, no. 11, pp. 21-27. 2018.
[72]. Hiroki Watanabe, Shigeru Fujimura, Atsushi and Jay (Junichi) Kishigami.. Blockchain Contract: A Complete Consensus using Blockchain., 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE). 2015.
[73]. Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland.. Decentralizing Privacy: Using Blockchain to Protect Personal Data., 2015 IEEE CS Security and Privacy Workshops. 2015.
[74]. Renita M. Murimi.. A Blockchain Enhanced Framework for Social Networking., Ledger Journal, 178, 2019.
[75]. F. Chen, R. Ji, J. Su, D. Cao, and Y. Gao.. Predicting Microblog Sentiments via Weakly Supervised Multimodal Deep Learning, in IEEE Transactions on Multimedia, vol. 20, no. 4, pp. 997-1007. 2018.
[76]. Wei W, Qi Y. Information Potential Fields Navigation in Wireless *Ad-Hoc* Sensor Networks. *Sensors*. 2011; Vol. 11, No. 5, pp.4794-4807, 2011
[77]. Xu, Q., Wang, L., Hei, X. H., Shen, P., Shi, W., and Shan, L., GI/Geom/1 queue based on communication model for mesh networks, *Int. J. Commun. Syst.*, Vol. 27, pp. 3013– 3029, 2014
[78]. Yang X L, Shen P Y, et al. Holes detection in anisotropic sensornets: Topological methods[J]. International Journal of Distributed Sensor Networks, Vol. 8, No. 10, pp.135054, 2012.
[79]. Qiang Y, Zhang J. A Bijection between Lattice-Valued Filters and Lattice-Valued Congruences in Residuated Lattices[J]. Mathematical Problems in Engineering, Vol. 36, No. 8, pp. 4218-4229, 2013.
[80]. Yang XL, Zhou B, Feng J, Shen PY. Combined energy minimization for image reconstruction from few views. Mathematical Problems in Engineering. 2012 Oct 31;2012.
[81]. H. M. Srivastava, Yunyi Zhang, Lei Wang, Peiyi Shen, and Jing Zhang. A local fractional integral inequality on fractal space analogous to Anderson's inequality[C]//Abstract and Applied Analysis. Hindawi Publishing Corporation, Vol.46, No. 8, pp.5218-5229, 2014.
[82]. Qi Yong. Information potential fields navigation in wireless Ad-Hoc sensor networks[J]. Sensors, Vol. 11, No.5, pp: 4794-4807, 2011.
[83]. Xu Q, Wang L, Hei XH, Shen P, Shi W, Shan L. GI/Geom/1 queue based on communication model for mesh networks. International Journal of Communication Systems. Vol.27, No.11, pp: 3013-29, 2014.
[84]. Yang X L, Shen P Y, et al. Holes detection in anisotropic sensornets: Topological methods[J]. International Journal of Distributed Sensor Networks, Vol.8, No.10, 2012.
[85]. Song H, Li W, Shen P, Vasilakos A. Gradient-driven parking navigation using a continuous information potential field based on wireless sensor network. Information Sciences, 408(C), pp: 100-114, OCT 2017.
[86]. H. J. Jie and P. Wanda, "RunPool: A Dynamic Pooling Layer for Convolution Neural Network," vol. 13, no. 1, pp. 66–76, 2020.
[87]. P. Wanda and H. J. Jie "DeepProfile: Finding fake profile in online social network using dynamic CNN," J. Inf. Secur. Appl., Vol.52, June 2020.
[88]. P. Wanda, Marselina Endah H, Huang J. Jie, "DeepOSN: Bringing deep learning as malicious detection scheme in online social network" IAES International Journal of Artificial Intelligence (IJ-AI), Vol:9, No:1, 2020.

[89]. Tobiyama, S., Yamaguchi, Y., Shimada, H., Ikuse, T. and Yagi, T., 2016, June. 'Malware detection with deep neural network using process behavior. In IEEE 40th Annual Conference on Computer Soft- ware and Applications, Atlanta, USA, June 2016, pp. 577-582.
[90]. Aslan, Ça r B. and Sa lam, Rahime Belen and Li, Shujun (2018) Automatic Detection of Cyber Security Related Accounts on Online Social Networks: Twitter as an example. In: 9th International Conference on Social Media & Society (SM&Society 2017), 18-20 July 2018, Copenhagen, Denmark, 2018.
[91]. Dadvar, M. and Kai Eckert. "Cyberbullying Detection in Social Networks Using Deep Learning Based Models; A Reproducibility Study." ArXiv abs/1812.08046 (2020).
[92]. Jha, S. et al. "Recurrent neural network for detecting malware." Comput. Secur. 99 (2020): 102037.
[93]. Masinde, N., Graffi, K. Peer-to-Peer-Based Social Networks: A Comprehensive Survey. SN COMPUT. SCI. 1, 299, 2020.
[94]. Wanda, P., Jie, H.J. DeepFriend: finding abnormal nodes in online social networks using dynamic deep learning. Soc. Netw. Anal. Min. 11, 34, 2021.

## Author Biographies

**PUTRA WANDA.** He received a Ph.D. Degree in the School of Computer Science and Technology, Harbin University of Science and Technology, China. His current research interests include Deep Learning, and Information Security. He has published several papers in conferences and journals indexed by Scopus, and SCIE (WOS). He is an invited reviewer in several high-impact journals including IEEE, Springer Nature, IGI Global, Wiley etc.
(email: wpwawan@gmail.com)

**Dr. (Cand) Rizka Ayu Setyani, SST, MPH** is a currently a student in Public Health Doctoral Program at Universitas Sebelas Maret, Indonesia through an outstanding alumni scholarship program. She is a lecturer and midwife who initiated and developed complementary midwifery therapy in Indonesia. She became the owner of Ayusofia Mother and Child Care and the founder of SEKOCI (Sekolah Komplementer Cinta Ibu, read: School of Complementary Therapy for Women). She collaborates with Public Health Centre in SEKOCI implementation and gets the best health inovator in Paragon Innovation Award 2021. She is a Prenatal Gentle Yoga Facillitator and Certified Mom and Baby Massage & SPA. She also works as a Public Relation in Tokoved, a digital company for health and tourism. Besides, she actively as a book author, consultant, speaker, and reviewer of journal.
(Email: rizkaayusetyani@student.uns.ac.id)

**IRMA PERMATA SARI.** She is a Lecturer in the Information System and Technology Department at Universitas Negeri Jakarta, Jakarta, Indonesia. Her current research interests include Machine Learning, Data Science, AR and Image Processing. Now, she is also as a Head of The IoT Laboratory, in Engineering Faculty. (email: im.irmapermata@gmail.com or irmapermatasari@unj.ac.id

**Niken Bayu Argaheni, SST, M.Keb**, is the author of the Essay "When Midwives Know the Gender Curriculum" (Winner of the 2nd Health Professional Education International Conference DIKTI in Bali, Indonesia), Kahlil Gibran's Essay in Indonesia published by the Lebanese Embassy, Essay in Khittah Journal "National Empowerment and the Reality of Microeconomics of NU", Article "Heteronormativity Communication between Health Workers and Spouses in the Child Care Process" Proceeding Book of the 1st International Conference for Midwives (ICMID) April 2016 and Oral Research Presentation Articles: "Relationship Between Gravidity and Lower Limb Vericose (International Public Health Conference in Colombo, Sri Lanka). HAKI: Application for Simulation of the Indonesian Alter Midwifery Competency Test. Can be reached at email: kinantiniken@gmail.com