Securing Sensitive Data Sharing in Web and Social Networks: A Dynamic Trust-based Approach

Shyam Prasad Teegala, PhD
Assistant Professor,
Department of CSE,
Anurag University,
Hyderabad, Telangana,
India

T. Shekar Reddy, PhD
Assistant Professor,
Department of CS,
Telangana Mahila Viswa Vidyalayam,,
University College for Women,
Hyderabad, Telangana,
India

T. Sunil Kumar, PhD
Assistant Professor,
Department of CSE,
Keshav Memorial Institute of Technology,
Hyderabad, Telangana,
India

Majeti Srinadh Swamy, PhD
Assistant Professor,
Department of AI,
Anurag University,
Hyderabad, Telangana,
India

ABSTRACT

Objective:
In this research, we aim to address the challenges posed by the surge in Security Method for Web and Social Network Applications. It is based on dynamic trust, focusing on the need to safeguard sensitive information amidst the dynamic nature of these platforms.

Method:
We developed framework for web and social network apps. This ensures security. It relies on dynamic trust for effective implementation. Users can trust their sensitive data sharing within this framework. This method utilizes innovative criteria for evaluating trust factors and employs dynamic trust assessments to adapt to the unpredictable behaviors of users within these platforms.

Findings:
Our investigation reveals that conventional static access control mechanisms are insufficient to mitigate the risks associated with data sharing in W-SNA. Through this implementation, we demonstrate the capability to effectively monitor and regulate negative behaviors, dynamically adjusting access levels to prevent inadvertent data disclosures.

Implications:
The adoption of DT-BSM offers significant implications for enhancing the security and confidentiality of data shared within W-SNA platforms. By empowering users to safeguard sensitive information effectively, this approach contributes to fostering a safer and more trustworthy digital ecosystem.

Conclusion:
In conclusion, our research underscores the importance of implementing a dynamic trust-based approach to address the complexities of data sharing in W-SNA environments. Through this adoption, users can navigate these platforms with greater confidence, mitigating the risks of breaches of confidentiality and misinformation dissemination.

Keywords
Dynamic Trust, web applications, Social networking apps

1. INTRODUCTION
Recently, online-based applications and social networks have gained popularity. Many sites are dedicated to finding and supporting links, finding and sharing different types of content. The development in the online Web and Social Networking Applications (W-SNA) show a new type of data network that is radically different from existing networks. It allows users and users to communicate and freely share information [1]. For example, links between content on the web pages a graph that is used to organize, direct, and organize data. It has gained great popularity and is a part of everyday life for many people around the world [2]. These are usually based on the idea that they build relationships with people they believe in. In such a scenario, it is possible to build up associations with individuals who have certainly not seen and still have common interests [3]. In addition, W-SNA has helped to expand public relations, which overcomes time and space constraints in many workplaces [4].

However, the extension of associations can lead to much harm, including invasion of privacy, sharing of data, and dissemination of misinformation. Therefore, it is natural to believe the credibility of informants, not information itself. People develop confidence in the process of sharing information [5]. In the W-SNA environment, several individuals keep their information in their area of interest for others to read or can update information on other information spaces. The data owner (DO) of the data may request the following requirements to monitor the access of other users. The DO will allow access to only trusted individuals to their domain. Before accessing the information, the information seeker may request permission from the owner. This step ensures proper authorization and respects the owner's rights. [6]. These needs in the W-SNA have been presented in access management programs such as "Mandatory access control" (MAC) [7], "Discrete access control" (DAC) [8], "Role-based access control" (RBAC) [9]. These conventional access control (AC) forms have restrictions when used in the W-SNA environment [10]. Since the user interface in W-SNA is constantly varying the constant regulations in normal input management are weak when using W-SNA. For example, a trustee who has broad access to information from the owner can become a malicious user who changes their passions, writes derogatory remarks, or reveals the DO's data. It is therefore significant for the DO to supervise the applicant's action regularly and ensure that it is trustworthy.

In the realm of web application services [11], trust is described as concerning the consumer's point of view, the application programs can give accurate outcomes and assure the non-working agreements. From the composer's perspective, the combined program must meet certain requirements, such as connectivity, accuracy, performance, and magnification [12], [13]. However, in a wide range of work atmospheres, fraud and

malware are frequently varied with truthful and high-quality things. An important area of research is how to differentiate untrusted programs from trusted programs and utilize trusted programs to generate additional applications [14], [15]. Considering the wide and dynamic nature of a web application service, it's essential to assess trust in atomic programs and integrated software. This proactive approach ensures security and reliability in your operations.

Trust typically demotes to circumstances considered by these characteristics: First entity (DO) is ready to trust in the functions of the other entity (user); the circumstances are prospect-oriented. Trust can depend on relationships between people [16]. W-SNA provides a great platform for users to share information, personal moments, thoughts, photos, and videos. Communication has evolved from point-to-point messaging to group activities among isolated users. W-SNA sites need to distinguish this key aspect of personal public relations and find well-structured and in-depth ways to implement it at the application level while giving the essential level of security, privacy, and trust [17].

While trust relationships need to be established and evaluated solely based on electronic communication over the Internet, the Internet is now being used for commercial, social, and educational relationships based on face-to-face relationships to establish trust relationships. A domain requires one domain to support different trust relationships and therefore can support different types of security management policies [18], [19]. W-SNA's secure mechanisms may include programs on other websites e.g. when it comes to assessing whether a person is genuine and trustworthy and not part of a joint fraud. When you join a social network, you start communicating with people who like to share information and build their trust system. This W-SNA does not take into account that some companions may be more secure than others.

Trust is typically described as DO among a trusted object, a target organization known as the user, that is, the target organization that emerges as an important aspect of the relationship in the web and social networks. be it for security, information access, or for use in advisory systems [20]. The use of W-SNA is rapidly evolving to share all sorts of social events. Since then, the sharing of information has also led to the possibility of security and privacy. It is always a big challenge to maintain appropriate privacy and AC schemes for the complexity of the relationships of many companions and team members [21]. In such cases, users are exposed to anonymous users and personal information that could be used to misrepresent or publish. Thus, preventing the anonymity of sensitive information is the foremost concern of this article.

This article presents Security Method for Web and Social Network Applications. It is based on dynamic trust and computation based on Simple Association Trust (SAT) by monitoring the type of actions and Past Trust (PT) identified and recommended by the companion s to compute an overall trust (OT). It will strengthen the trend and relationship between DO and the user in terms of the trust. It provides a User Data Access Manager (DAM) that acts as a requestor and supervisor to operate the method, to assess the trust, and provide an entry-level based on the current DT calculation. The entry-level is based on the user's DT value. In addition, the proposed method will provide a mechanism for updating confidence levels and identifying malicious user actions, and maintaining user privacy.

This article is sorted as follows. Section 2 outlines the security requirements and limitations of the conventional W-SNA mechanism. Section 3 shows how to calculate a dynamic trust-based security method. Section 4 shows the results of the tests in different scenarios and the results of this paper in Section 5.

2. RELATED WORKS

The usage of the Web and Social Networks is a part of everyday life for many people. Many W-SNA contributors such as Amazon, Wiki, WhatsApp, and Twitters have used AC methods to control the stream of information and avoid confidentiality. From an association point of view, the individual user shares their relationship with their companions, family, and colleagues. From an information point of view, sensitive information can be divided into public, personal, or individualized groups. These AC methods are depending on conventional static AC methods [6], [8], [9], [10], [23]. However, the security mechanisms in social networks are changing, but the concept is almost always the same: When you join a social network, you start communicating with people who like to share information and build their trust system. Privacy settings vary among social networking sites, but there has been a debate in the media about privacy settings that allow people outside the social network to access their personal information [24]. Sometimes someone on this social network must do something with it and that person's companion - a multi-hop user - receives information about the action. However, this can lead to unwanted situations and the user needs to know how to approach the privacy settings.
Trust is extensively acknowledged as a fundamental part of individual social relations [12], [13]. Confidence in psychology is considered to be the psychological state of DO, where there is a risk of positive beliefs of the user's action [5], [25]. It can be defined as "the subjective expectation of one organization for the future of another." In W-SNA, the two main players of trust are divided into groups as DO and user. A particular trust value is accumulated based on earlier actions or experiences, and utilizing this trust decides whom to allow and whom to restrict.

Several studies on trust have been conducted in the past [14], [17], [18], [21], [26] to reduce the uncertainty and risk of future relationships between DO and the user. The DO evaluates user credibility if they know how to do a DO, but evidence that there is important communication and exchange of information between anonymous individuals in the W-SNA atmosphere is of great concern to the sensitivity of the data and the privacy of the user.

Calculating the value of trust is considered a subjective probability. Mui et al. [32] define trust as subjective anticipation, which is the agent's probability of the future action of others following their past actions. The trust of an organization depends on its reputation. . It is the user expectations for the performance and capabilities of complex services. This is considered a priority as it may be updated or adjusted periodically. It can give punishment and rewards for preventing unauthorized service delivery and trust monitoring [6]. Several concerns and limitations related to reliability management are described in [13], [14], [18]. Trust and reliability necessitate being updated and evaluated efficiently. To accomplish that, we need to aim at enhancing the algorithms and procedures for trust calculation and service provisioning.

2.1 Security Requirements in W-SNA

Security risks have increased as W-SNA has evolved into an important online communication platform that is incorporated into individuals' everyday lives. As social networks grow in popularity, hackers, scammers, and malicious users can use them as an attack vector for traditional cybercrime, launch specific attacks on social networking users, or launch them directly and begin to commit illegal acts or do attacks to interrupt web applications or social networking sites. W-SNA has some unique characteristics that make it ideal for abuse by online criminals. It is a massive, extremely distributed consumer base made up of clusters of consumers who share common social attentions and build mutual beliefs.

Malicious users or groups create fake compliments or biased references as recommendations. In the Sybil kinds of attack [34], one individual personalizes several personalities. For example, an attacker by voting a user profile account as "excellent" to increase the visibility and reputation rating of an individual for the availability for e-business. A malicious pre-trusted peer is able to oppose DO later beginning an association and influencing the trust value of DO for the recommender systems. While the new paradigm offers many opportunities, it can play a role in hindering growth and user recruitment when implemented without considering the required security requirements. In addition, social networks are a highly desirable target for large attackers, as they attract thousands of potential users. Table 1 shows the attacks on W-SNA related to trust.

Table 1: Attacks related to trust in W-SNA.

Case	Attacks
Privacy	The accessibility of critical information on W-SNA provides a safe environment for users to misuse and exploit that information. Unauthorized disclosure of confidential information can be an excellent prospect for illegal and fraudulent acts to carry out illegal data mining activities in W-SNA. Malicious attackers can use obscene material and confidential data from W-SNA to choose targets, profile losses, and preparation to perform several cybercrimes conducts.
Malicious code	The malicious code uses the accounts of infected users of W-SNA to gather users' information and distribute useful information. Additionally, many attackers use W-SNA media to produce bogus profiles and expose deceptive links to sites compromised with malicious code. They usually utilize several modes to acquire this sensitive information such as advertisements, prizes, download links, etc., as the online users base is increasing every day. Even
Safety and Criminality	W-SNA atmospheres pose a severe threat to adolescents and young children as they can fall prey to multiple attacks such as getting popularity, online games, attractive offers, and easy earning money. In general, the most common forms of child attacks on W-SNA websites are those of peers, young people, and the elderly. Due to the huge number of users and the fact that not all users use real identities, the providers are struggling to get rid of the web
	links completely.

Social network providers are like other web applications which might be highly vulnerable to direct attacks. The vulnerabilities of the W-SNA give a way for hackers to attack and acquire unlawful user credentials leading to service failures. In addition, it can be utilized by a bug and spread to consumer accounts. In W-SNA the users are majorly vulnerable to XSS (cross-site scripting) or SQL injections, which has impacted many business applications in the past.

2.2 Related Trust Assessment Mechanism

A method for assessing trust based on indicators of trust in reputation and knowledge is proposed in [28]. According to the trust sharing service, there are numerous elements for analyzing and managing trust, as well as a trust model. A proficient scheme for predicting trust for “service-oriented W-SNA” is shown in [29]. The author identifies two existing problems related to the forms of the spread of trust in the context of W-SNA. Primarily, it states that W-SNA is generally huge and scalable. The problem of building trust in such networks takes a long instance and, secondly, optimizes the spread of trust. To solve these problems, they proposed using the link between center-level distribution and the distribution of trust on social networks, as well as the use of hubs (contact between applicant and supplier) to spread trust.

Hu et al. [20] and Yuan et al. [25] proposed a multi-party and user-to-user relationship control approach for W-SNA. The consumer may have relatively multiple roles such as DO, data reader, data updater, and distributor. In these roles, there is a defined approach that can be computed using weighted assessments. The result of the computation influences the resolution to allow access to the information. Alternatively, these benefits include resolving disputes among consumers about policies. The consumer must configure each of the role-based information sharing policies before being allowed. This is able to be complicated when changing policies.

Shan et al. [30] proposed an SVM algorithm was to implement an integrated intelligent AC method (SVM-SAC) that relies on the association kind and the description information of the substance disclosed as a characteristic vector. It aims to provide solutions for more associates and difficult associations, making it additional complicated to create AC policies for W-SNA users. SACM-SVM can routinely suggest a collection of noticeable companions, depending on the substance circulated by consumers and the association among consumers and mates, allowing consumers to adapt the collection to acquire the newest AC strategy that can efficiently shield consumers' confidentiality data.

Voloch et al. [31] propose a novel responsibility and trust-based AC method, called "RTBAC". In this model, various privilege explicit roles are allocated to consumers united to the self-worth node, and all users are evaluated for trust. By some criteria, such as the total number of companions, age of consumer account, duration of companionship, etc. This is a combination of user trust attributes based on the actual W-SNA characteristics within RBAC, which normally grants authorizations only to functions, thereby getting better the confidentiality capabilities of the network. These can improve the information-sharing decisions made by W-SNA. Experimental evaluations strongly demonstrate the legitimacy of the confidence calculation form and its feature threshold

factors.

Shan et al. [32] propose a HAC (hybrid access control model) for W-SNAs that use properties and associations to monitor the availability of these resources. A novel strategy condition language has been the build-up to determine the policy, taking into account the associations and characteristics of the consumers. A roadmap procedure is suggested to determine if the roads between the two users can be compliant with the hybrid policy. A prototype is employed and many types of research are assessed to verify the probability of the method. HAC has advantages over existing W-SNA AC methods in periods of policy language self-expression and access request evaluation algorithms.

Cheng et al [33] suggested a UURAC (user-to-user relationship-based access control) form for W-SNA schemes that use standard term information for such strategy requirements. It provides "DFS" and "BFS" based route control procedures and evaluated the complication of the procedures. The demonstration of the two algorithms and the results of the evaluation have demonstrated the probability of our mechanism by considering the evidence. It confirms the possibility of the mechanism by introducing a system model and estimates the execution of these two procedures.

Carminati, et al. [35] proposed an input control model based on a rule that regulates input data by the type of relationship, the depth of the relationship, and the value of trust. In particular, every trust assessment given to an individual is constant and subjective. However, when used in the current W-SNA environment, these trust criteria are problematic since consumer associations are constantly altering and consumer trust is not defined in W-SNA. In addition, they get used to the consideration of trust, which means that companions are safe.

There are different criteria for evaluating trust and different evaluation methods. Continuous or separate assessments are used to measure confidence levels. For example, trust is defined as confusing logic, and probability models [13], [21] and [8], [17], [27] are also used to measure trust. Several researchers measure trust depending on a collection of QoS features [36]. In other terms, this is done according to a set of QoS features such as cost, availability, trustworthy and reaction instance to find the best connection scheme with the highest QoS value. After all, finding the most suitable connection plan for NP is a very difficult task and it takes considerable time and attempts to locate the most suitable connection arrangement. Traditional algorithms have also been personalized to the domain of trusted search engine optimization to find the best connection scheme for solving NP-critical issues such as simple linear, dynamic programming, and key problems [37].

There are many disadvantages to using conventional and constant input management methods as explained above. Primarily, it is complicated to alter access procedures before correcting consumer access. Secondly, it is not practical to employ a relationship-based AC method to the dynamic environment of W-SNA, as associations alter recurrently. Finally, a trusted consumer can be harmful to other consumers. Therefore, it is essential to use a dynamically adapted trust-based security mechanism in W-SNA.

3. PROPOSED METHOD

The functional design of the proposed method is shown in Fig. 1 to provide the W-SNA. It mainly consists of two basic modules for controlling user access to information and user attacks such as Data Access Manager (DAM) and Dynamic Trust Computing.

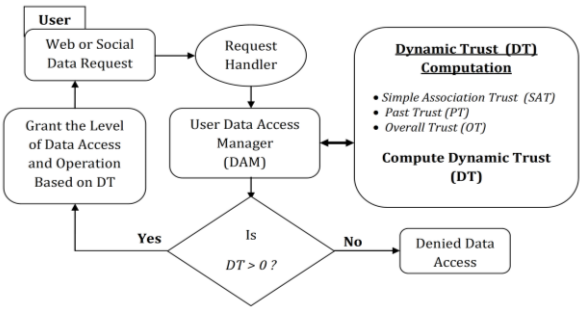

Fig.1: Information flow and control in proposed method

When the user requests information, the software developer in the middleware interacts with the DAM to determine the possible trust value of the user. The value of user trust was calculated as dynamic trust (DT) based on simple association trust (SAT), previous trust (PT), and overall trust (OT). If the user has a DT value > 0, it is based on the DAM access control configuration for the level of access to information to allow for possible malicious actions and attacks.

3.1 Data Access Manager (DAM)

Communication on W-SNA is different from communication offline because it doesn't have a physical relationship with its companions or assistants and there is no limit to the amount of knowledge it can only see unfamiliar features. But testing trust can direct to better associations between individuals, even though they didn't know each other exactly. The assessment of trust is the extent to which the subjects determine the function of the likely act in a given circumstance. The presented model uses the perception of trust by predicting the user's past action and detecting future action. Relationships and ongoing associations allow the consumer to anticipate future actions and the relationship means more trust.

The DAM plays the role of providing user access control. It restricts other operations when the user is asked for access. Thus, a static environment is guaranteed in a dynamic W-SNA environment to ensure the trust is correct. As shown in Table 2, the DAM mechanism is divided into groups for the DO, the user, and the third-party, which provides indirect trust based on the specified limit of the value of the applied trust to determine the allowable level with the attack.

Table-2: DAM Access Management Configuration

Level of Access Grant	Probable Range of DT value	Granting functions access	Reorganization of Probable Attacks
0	0	Ø	None
1	0.1 and < 0.4	{only read}	Passive recognition of information
2	0.4 and < 0.6	{read and status update (like or	Passive action against information

		dislike)}	
3	0.6 and < 0.8	{ read, status update and remark}	Malicious reaction against information
4	> = 0.8	{ read, status update, remark, tag and sends information }	Exploit dynamic malicious of the DO's and domain

The DO is a subjective organization that must determine whether or not access request data is allowed. The user must be confident enough to get access to the DAM. The DAM module is responsible for reliably calculating the user that provides the DT value by calculating the current and previous trust estimates. The process of calculating the DT will be discussed in the next section.

3.2 Process of Dynamic Trust (DT) Computation

The trust calculation process gives the user the degree of the grant of entry to the DT relies on the outcome of the computation. Trust is a dynamic variable in the W-SNA environment. Competitors, such as malicious consumers or previously trusted consumers, might modify their preferences and happen to malicious consumers in potential deals with DOs. However, it is hard to identify a change in the applicant's intent to access the data. As a result, trust assessment should be based on regular monitoring of operations and customer activity. To calculate the DT, the user first calculates the SAT and PT and then calculates the OT using both. As a result, OT and other influential factors calculate the user's DT value.

3.2.1. Computation of Simple Association Trust (SAT)

A DO is fulfilled once a user accesses and utilizes the DO's information as expected. That is, DO's trust is the DO's sensitivity to observation as DO based on the user's positive feedback as *U*. Trust is defined as a DO's as *SAT* beside the user since trust is subjective depending on the direct practice in user's action. It implements the narrative of trust DO's trust association based on its capability as *C*, maintainability as *M*; whereas for the user it will be association bonding as *B* between others users in relations. The action of the two entities which affects their trust association is given in Table-3 below.

The computation of SAT utilizing the factor *C*, *M*, and *B* according to the DO and user trust tendency criteria is defined with a unifying factor as *tc* for *Trust capability*, *tm* for *maintainability*, and *tb* for *Trust bonding.* Based on these factors it derives the computation of SAT as given in Eq. (1),

$$SAT(DO,U) = (C \times tc) + (M \times tm) + (B \times tb) \quad (1)$$

where, the range of value of *tc*, *tm*, and *tb* lies between 0 and 1, and it summation these three factors always will be 1, (*i.e. tc + tm + tb =1*). The value of *C*, *M*, and *B* varies according to the *+ve* and *-ve* actions similarity association given in Table-3. So, the stage of SAT is symbolized by the measure of *SAT(DO,U)*, where $0 \leq SAT(DO, U) \leq 1$, in addition to zero, indicates that the DO's trust beside the user is completely unreliable and one is completely trustworthy**.** As per the user's actions changes over time *t* the value of trust also varies. So, after a set of action observations in *t* interval is computed as given in Eq. (2),

$$SAT(DO,U)_t = (1-\omega) \times SAT(DO,U) + \omega \times SAT(DO,U)_{t-1} \quad (2)$$

where, "ω" → the affecting rate of the earlier *SAT*, and "$t-1$" → the previous operation.

Table-3: Trust Association Factor and Actions

Object Entity	**Trust Association Factor**	**Description**	**Type of Actions**	
			+ve	***- ve***
Data Owner (DO**)**	Capability (C)	Features that allow the user to interact within a precise area. The user may be more proficient in the DO's area, which indicates that he or she believes in issues related to the area.	Like, link, and share	Dislike
	Maintainability (M)	The idea of a user who wants to log in to someone's area regularly.	Likes, remarks, respond and chat	Mishandling information
User (U)	Bonding (B)	Definite relationships among more than two individuals who connect to a well-built or a weak connect.	Companionship, number of frequent associations.	Obstruct associations.

3.2.2. Past Trust (PT)

SAT calculations are presented by tracking earlier operations. If the user is unidentified, a trust association can be recognized by setting a default cost. It thinks that two consumers who do not identify with each other are ready to work together. Data owners have difficulty sharing information with unknown users. Generally, the information holder asks his or her companion s about the applicant. For instance, "*User1*" and "*User2*" are companions, and "*User2*" and "*User3*" are companions. So, indirectly "*User1*" and "*User3*" are companions. The association between "*User1*" and "*User2*" is well-known as they are direct contact. But, it might possible

"*User1*" trust "*User2*" but might not "*User3*". It is possible "*User2*" can share sensitive or confidential information with "*User3*" as it has a direct association with "*User2*". In [28] author advises the process of computing PT. It describes that PT is computed as an average SAT measure of third parties having past trust experiences of the users. The level of trust measure is computed with close monitoring of user earlier experiences.

To initiate calculating the PT, the DO needs to recognize the resemblance of another DO against the user. Individuals are more secure when they assemble other individuals who have related features. In addition, comparisons affect companionship, and individuals with common companionship become closer to each other.
Similarities are the level at which individuals have similarities in the way they estimate trust. Therefore, it estimates the similarity based on frequent companions and their SAT obtained from Eq. (2). The average isolation ($Avg_{isolation}$) among the DO and user is computed using Eq. (3) as given below.

$$Avg_{isolation}(DO,U)_t = \frac{1}{F}\sum_{n\in F}\frac{1}{SAT(DO,n)_t \times SAT(U,n)_t} \quad (3)$$

where *F* represents the number of frequent companions (*n*) among the *DO* and *U*. It utilizes a "BFS (breadth-first search)" procedure to find out frequent companions with the smallest route (means the closest trust) [16].The $Avg_{isolation}$ shows an enhancement or reduction in the comparison of similarity. The association similarity (A_{sim}) enhances when the standard satisfaction gap is lower than the threshold of gap (τ) and reduces when the gap among them is higher than τ.

Das et al. [38] employed the perception of punishment (β) and reward (α) coefficients for computing of A_{sim}. It fixed a higher β coefficient, because of the complexity to ascertain trust which makes to drop trust quickly. Hence, A_{sim} is determined as,

$$A_{sim}(DO,U)_t = \begin{cases} A_{sim}(DO,U)_{t-1} + (\alpha \times (1 - A_{sim}(DO,U)_{t-1})), \\ \text{where } \mathrm{Avg}_{isolation}(DO,U)_t < \tau \\ A_{sim}(DO,U)_{t-1} - (\beta \times (1 - A_{sim}(DO,U)_{t-1})), \\ \text{where } \mathrm{Avg}_{isolation}(DO,U)_t \geq \tau \end{cases} \quad (4)$$

where $0 < \alpha < \beta < 1$ and $0 \leq A_{sim}(DO, U) \leq 1$. It assumes that $Avg_{isolation}(DO, U)_t$ is *0*, when no companions are similar among the DO and user, and the preliminary A_{sim} is *0.5* as the average of trust.

In determining the $Avg_{isolation}$ DO demands the data concerning to the user from his companions who have had earlier familiarity with the third-party. It utilizes a standard measure of the entities of the third-party's *SAT* and A_{sim} to conclude the PT. So, the PT is computed using the Eq. (5) as,

$$PT(DO,U)_t = \frac{\sum_{k\in adj(O)} SAT(k,U)_t \times A_{sim}(k,U)_t}{|k|} \quad (5)$$

where $k \in \mathrm{adj}(O) \rightarrow$ that the third-party is closest to the DO and it has earlier trust knowledge with the user.

3.3 Compute Dynamic Trust (DT)

A linear permutation among the *SAT* and *PT* measure at the t^{th} operation gives the overall trust (OT) utilizing the Eq. (2) and (5). So, the computation of the *OT* of S to P as,

$$OT(DO,U)_t = \gamma \times SAT(DO,U)_t + (1-\gamma) \times PT(DO,U)_t \quad (6)$$

where, γ represents the affecting rate of the *DT*, and $0 \leq \gamma \leq 1$.

In place of a suitable fraction of *SAT* and *PT*, it employs the γ that assured the lowest deviation relation of SAT and *r*. This is regulated as per the operation rate among the DO and user as,

$$\gamma = \begin{cases} r, \text{ where } \gamma < \mathrm{r} \\ r + \dfrac{\sum \text{number of operations (DO, U)}}{\sum_{p \in \mathrm{P}} \text{number of operations (DO, U)}}, \\ \text{where } \gamma \geq \mathrm{r} \end{cases} \quad (7)$$

where $P \rightarrow$ is a collection of individuals who have earlier trust knowledge with the user.

As revealed earlier, the trust measure transforms and progresses with earlier trust knowledge. So, utilizing the Eq. (6), DT is computed as,

$$DT = (1-\rho) \times OT(DO,U)_t + \rho \times OT(DO,U)_{t-1} \quad (8)$$

where ρ is the deviation rate of the PT value.

4. EXPERIMENTAL EVALUATION

4.1 Setup

An experimental evaluation was carried out utilizing the Java development APIs and an influenced illustrative package to test the performance of the DT-BSM developed for AC. It used a subsystem of 255 units and 1,280 edge datasets given by the University of Princeton [39]. The preliminary configuration of the factors utilized in the trust computation is given in Table-4.

Table-4: Configuration of Trust constants factors

Factors	Contents	Value
τ	Average distance threshold	0.20
α	Reward coefficient	0.04
β	Punishment coefficient	0.08
ω	Deviation rate of SAT	0.20
r	Deviation rate of the minimum ratio of SAT	0.20
ρ	Deviation rate of PT	0.5

4.2 Result Analysis

The experiment process is initially performed to analyze the change in DT to change the operation. It then evaluates the different users with different DT and access grant levels and finally compares the proposed DT-BSM with the AC methods available in the W-SNA for malicious users.

A. Analysis of DT with varying different actions

There are two perfect circumstances in which users carry out regular observation of positive actions and negative actions. It randomly opts for two users in the test and examines the changes in user trust.

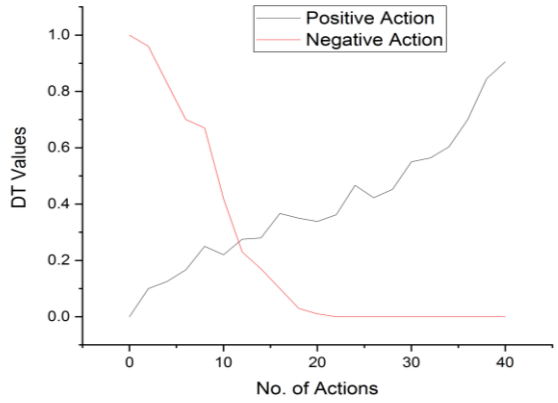

Fig. 2: DT variation with the increasing number of actions

Fig. 2 shows the results of varying confidence values with different behavioral conditions. It has eroded the confidence of one user (positive action) because trust must be accumulated as described in Section 3 above. In addition, it is difficult to trust others who do not have a user experience. However, as the user continued to show positive action, trust increased gradually. In contrast, it put the remaining user's opening trust in 1, but these nodes might be with negative actions. This shows that negative action has led to a significant reduction in trust. The analysis outcome reveals that trust was constructed gradually even though it turned down rapidly.

B. Analysis of DT with varying Access Level condition

It is supposed that a user can select a calculated action and modify his or her situation in a loop of the 100th operation, i.e., between 0 to 100th operation, with negative approval for consequent 100th operations. It hypothesized that the highest and lowest values would constraints the 100th operation as malicious users may have a focus on persistent actions on the aim user for a small term [15]. It has mapped DT calculation results with access level permissions. This indicates that the satisfactory operation of the user has increased the level of access, thus expanding the scope of the operation available in the user's domain. Fig. 3 shows the dynamic change analysis of DT for the user's access level condition.

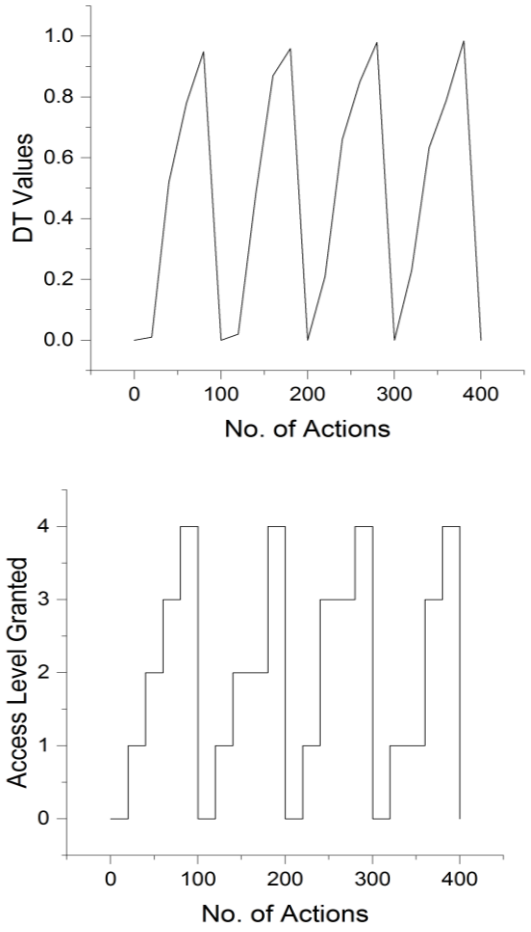

Fig. 3 (1)(2): Variation of DT and Access level with the number of actions

For instance, executing continuous acceptable actions directs to the sharing of other data. In opposition, malicious or unacceptable actions reduce the level of AC and decrease access to the content of the DO. Even if a trusted companion is asked for information, harmful actions such as leaking different information can be easily detected and protected.

C. Analysis Security success rate with varying Non-Trust Users

As described in Section 2, it can monitor typical attacks such as Sybil attacks, sets of malicious users, and malicious pre-trusted users. Malicious, pre-trusted peers can choose positive or negative actions depending on the user's choice. In addition, Sybil attacks consist of multiple users with identical ID and action tendencies, with malicious groups taking negative actions for a set of users. Therefore, assuming the attack situations every 10 times the simulation was performed.

We have segregated every user into two sets in the form of a trusted set with non-malicious users and a trusted set with malicious users. Every set performed a dynamic action depending on the level of trust. For example, users in a malicious group were initially assigned a low trust access level, increasing their chances of misbehaving in the DO domain. The proposed DT-BSM model was determined in comparison to the earlier AC methods as SVM-SAC [30], RTBAC [31], HAC [32], and UURAC [33] with properly controlled permissions.

Fig. 4 shows the percentage of the average number of operations allowed to a user based on reliability. According to the user's DT, the probability level of access is given by DAM. The higher the confidence, the more operations are tolerated. Traditional AC methods maintain a certain level of reliability after a particular operation period, allowing access to an operation. At this stage, it retains the state of the operation that the untrusted user uses to execute the malicious operation. However, in the proposed DT-BSM model, the DT value changes dynamically and the trust level is periodically reconfigured to zero each time the user is forced into the 100th operation. As the level of DT value decreases, so does the level of operations are allowed to control the DO's data privacy.

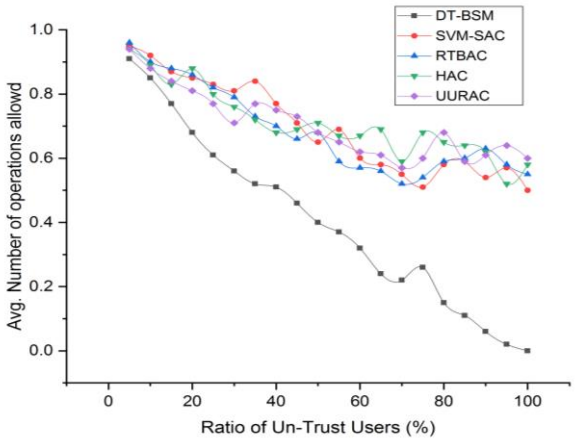

Fig.4: Comparison Analysis of operation preserving with varying un-trusted users.

5. CONCLUSION AND FUTURE WORK

This paper described the calculation of DT and its service granting levels that define the scope of users in W-SNA access. W-SNA builds dynamic network setting, with elements such as roles, content, and profiles constantly varying. Trust is utilized as a platform to resolve the limitations of traditional constant AC mechanisms at present taken up by W-SNA such as online shopping, ticket booking, WhatsApp, Twitter, and Facebook. The proposed DTBSM demonstrates that data owners can manage and defend informal or malicious data leaks and control untrusted users from malicious information sharing in social network applications. It presents a DAM with a DT calculation method by measuring the trust of a user's simple association and the trust of the past. This simplifies the complexity of managing access decisions with DO and social applications and takes action in a W-SNA environment. Experimental analysis with varying user DT values and access levels for positive and negative actions filters untrusted users from the W-SNA environment. A comparative analysis of past methods with distrust of different users shows effective control of operation preserving. As a future extension, analysis of positive and negative action classifications to reduce the complexity of assigning access decision levels and maintain access control schemes from anonymity through web application authentication.

6. REFERENCES

[1] G. Aydin, N. Uray, G. Silahtaroglu, "How to Engage Consumers through Effective Social Media Use—Guidelines for Consumer Goods Companies from an Emerging Market", Journal of Theoretical and Applied Electronic Commerce Research, Vol. 16, pp. 768–790, 2021.

[2] S. Patil, Pratiksha. " A Secure Data Evaluation and Publishing Technique for Big Data" International Journal of Computer Applications (IJCA) 975:8887

[3] S. Tripathi, S. Verma, "Social media, an emerging platform for relationship building: A study of engagement with nongovernment organizations in India", International Journal of Nonprofit and Voluntary Sector Marketing, Vol. 23(1), 2018.

[4] S. H. Webb, S. J. Roberts, "Communication and social media approaches in small businesses", Journal of Marketing Development and Competitiveness, Vol. 10(1), 2016.

[5] F. Li, H. Li, B. Niu, and J. Chen, "Privacy computing: Concept, computing framework, and future development trends", Engineering, vol. 5, no. 6, pp. 1179-1192, 2019.

[6] Y. G. Wu, W. H. Yan, J. Z. Wang, "Real identity based access control technology under zero trust architecture", Int. Conference on Wireless Communications and Smart Grid (ICWCSG), 2021.

[7] S. Achleitner, Q. Burke, P. McDaniel, T. L. Porta, "MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking", Networking and Internet Architecture, arXiv:2009.10021v1, 2020.

[8] S. Kaushik, G. Charu, "Capability Based Outsourced Data Access Control with Assured File Deletion and Efficient Revocation with Trust Factor in Cloud Computing", International Journal of Cloud Applications and Computing (IJCAC), Vol.10(1), pp.64-84, 2020.

[9] C. Blundo, S. Cimato, L. Siniscalchi, "Managing Constraints in Role Based Access Control", IEEE Access, Vol. 8, 2020.

[10] X. Jin, R. Krishnan, and R. Sandhu. "A unified attribute-based access control model covering DAC, MAC and RBAC", In IFIP Annual Conf. on Data and App. Security and Privacy, pp. 41–55, 2012.

[11] O. Ochoa, M. Rodney, N. D. Rio, "Accessing Provenance Records in Semantic Web Services", IEEE 14th International Conference on Semantic Computing (ICSC), 2020.

[12] S. Rouhani, R. Deters, "Data Trust Framework Using Blockchain Technology and Adaptive Transaction Validation", IEEE Access, Vol. 9, 2021.

[13] Y. Wang, X. Tong, "Trust Prediction Based on Extreme Learning Machine and Asymmetric Tri-Training", IEEE Access, Vol. 9, 2021.

[14] S. Hussain, R. A. Naqvi, S. Abbas, M. A. Khan, T. Sohail, D. Hussain, "Trait Based Trustworthiness Assessment in Human-Agent Collaboration Using Multi-Layer Fuzzy Inference Approach", IEEE Access, Vol. 9, 2021.

[15] F. Shang, W. Wu, Y. Gu, "A unified model of RBAC and DAC", IEEE 2nd Int. Conf. on Art. Intelligence, Management Sci. and Electronic. Commerce (AIMSEC), 2011.

[16] X. Liu, J. Fu, "SPWalk: Similar Property Oriented Feature Learning for Phishing Detection", IEEE Access, Vol. 8,

2020.

[17] G. D. Putra, V. Dedeoglu, S. S. Kanhere, R. Jurdak, A. Ignjatovic, "Trust-Based Blockchain Authorization for IoT", IEEE Transactions on Network and Service Management, Vol. 18(2), 2021.

[18] Y. G. Wu, W. H. Yan, J. Z. Wang, "Real identity based access control technology under zero trust architecture", IEEE Int. Conference on Wireless Comm. and Smart Grid (ICWCSG), 2021.

[19] K. Sohr, M. Drouineaud, G.-J. Ahn, M. Gogolla, "Analyzing and Managing Role-Based Access Control Policies", IEEE Transactions on Knowledge and Data Engineering, Vol. 20(7), 2008.

[20] H. Hu, G.-J. Ahn, J. Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms", IEEE Transactions On Knowledge and Data Engineering, Vol. 25, No. 7, 2013.

[21] S. M. Ghafari, A. Beheshti, A.Joshi, C. Paris, S. Yakhchi,M. A Orgun, A. Jolfaei, Q. Z. Sheng, "Modeling Personality Effect In Trust Prediction", Jr. of Data Intelligence, Vol. 2(4), pp. 401-417, 2021.

[22] S. Gustafsson, N. Gillespie, R. Searle, V. H. Hailey, G. Dietz, "Preserving Organizational Trust During Disruption" Organization Studies, Vol. 42(9), pp.1409–1433, 2021.

[23] P. W. L. Fong, M. Anwar, and Z. Zhao, "A privacy preservation model for facebook-style social network systems", in Proc. Eur. Symposium. Resarch Computing Security, pp. 303-320, 2009.

[24] T. Phillips, X. Yu, B. Haakenson, and X. Zou, "Design and implementation of privacy-preserving, flexible and scalable role-based hierarchical access control". In 1st IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), pp. 46–55, 2019.

[25] C. Yuan, J. Park, and R. Sandhu, "A user-to-user relationship based access control model for online social networks", in Data and Applications Security and Privacy, vol. 26, pp. 8-24, 2012.

[26] H. Nusantoro, R. Supriati, N. Azizah, N. P. L. Santoso, S. Maulana, "Blockchain Based Authentication for Identity Management", IEEE 9th Int. Conf. on Cyber and IT Service Management (CITSM), 2021.

[27] L. Mui, M. Mohtashemi, and A. Halberstadt, "A computational model of trust and reputation", in Proc. 35th Int. Conference System Science, pp. 2431-2439, 2002.

[28] N. B. Truong, T.-W. Um, G. M. Lee, "A reputation and knowledge based trust service platform for trustworthy", in Proc. 19th Int. Conf. Innov. Clouds, pp. 104-111, 2016.

[29] Y. Xu, J. Liu, M. Tang, and X. F. Liu, "An efficient trust propagation scheme for predicting trustworthiness of service providers in service oriented social networks", in Proc. IEEE 20th Int. Conf. Web Services, pp. 467-474, 2013.

[30] F. Shan, J. Liu, X. Wang, W. Liu, B. Zhou, "A Smart Access Control Method for Online Social Networks Based on Support Vector Machine", IEEE Access, Volume: 8, 2020.

[31] N. Voloch, P. L. M. Elmakies, E. Gudes, "An Access Control Model for Data Security in Online Social Networks Based on Role and User Credibility", International Symposium on Cyber Security Cryptography and Machine Learning(CSCML), pp 156-168, 2019.

[32] F. Shan, H. Li, F. Li, Y. Guo, Ben Niu, "HAC: Hybrid Access Control for Online Social Networks", Security and Communication Networks, Article ID 7384194, pp. 11 pages, 2018.

[33] Y. Cheng, J. Park, R. Sandhu, "An Access Control Model for Online Social Networks Using User-to-User Relationships", IEEE Transactions on Dependable and Secure Computing, Vol. 13(4), 2016.

[34] Y. Zheng, Z. Li, X. Xu, Q. Zhao, "Dynamic defenses in cyber security: Techniques, methods and challenges", Digital Communications and Networks, 2021.

[35] B. Carminati and E. Ferrari, "Enforcing relationships privacy through collaborative access control in Web-based Social Networks", in Proc. 5th Int. Conf. Collaborative Computer Network, pp. 1-9, 2009.

[36] W. Li, J. Wu, Q. Zhang, K. Hu, and J. Li, "Trust-driven and QoS demand clustering analysis based cloud workflow scheduling strategies", Cluster Computing, Vol. 17(3), pp. 1013-1030, 2014.

[37] Y. Wang, I.-R. Chen, J.-H. Cho, A. Swami, and K. S. Chan, "Trust-based service composition and binding with multiple objective optimization in service-oriented mobile ad hoc networks", IEEE Transaction Services Computing, Vol. 10(4), pp. 660-672, 2017.

[38] A. Das and M. M. Islam, "SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems", IEEE Transactions on Dependable and Secure Computing, Vol. 9(2), pp. 261–274, 2012.

[39] "Dataset", http://algs4.cs.princeton.edu/43mst/mediumEWG.txt.