Volunteer Management System for Disaster Management

Noor Afiza Mat Razali, Nurjannatul Jannah Aqilah Md Saad, Hasmeda Erna Che Hamid, Muhammad Ramzul Abu Bakar, Khairul Khalil Ishak, Nor Asiakin Hasbullah, Norulzahrah Mohd Zainudin, Suzaimah Ramli, Norshahriah Wahab

ABSTRACT--- Based on the National Security Council (NSC) Directive No. 20 that concern in coordinating responsible agencies and committee, the Malaysian government have established a disaster management coordination and preparedness agency. During disaster relief and operation, volunteer involvement also can be an important part of disaster relief. Researchers are proposing the usage of the systematic volunteer management system (VMS) to manage volunteer activities on the scene by optimizing volunteer involvement. This study provides an overview of VMS and its challenges, focusing on the process of volunteers' recruitment and management of volunteers' personal information that needed to be handled according to the information security concept which is privacy, security, accessibility and control of that information. This paper proposes VMS design for Malaysia and reviews security apprehension which also includes concern on trust issues that may arise between government coordination agencies and the volunteers in managing sensitive information either from government agencies or volunteers side. The proposed VMS include the concept of trust and the implementation of security by design concept at the development phase.

Index Terms— Disaster management, information security, volunteer management system.

I. INTRODUCTION

Disaster has been classified into two types which man-made disaster or natural disaster. Natural disaster is usually termed as the 'Act of God' such as flood, earthquake, landslides and many more which men can't control or handle.As for man-made, it is usually an incident that can cause a socio-technical disaster [1].Man-made disaster is an incident that can cause a socio-technical disaster that includes acts of terrorism, explosion or leakage in critical national infrastructures such as water, gas and electricity facility. The advancement of communication technology resulted in efficient information sharing about disaster and triggering a large number of people and groups that not affiliated with traditional emergency response organization to offer for their assistance during a disaster crisis phase. At this phase, despite having highly specialized relief rescue team, the volunteer is also part of disaster relief as they are the first respondent to react to such situation as they are usually the first to be on the scene [2]. In most developed country, emergency and disaster management highly rely on the workforce of professional personnel and volunteers that affiliated with local authorities or agency [3]. As an example, Florida emergency management professionals making volunteers as part of relief and emergency plan whereas they always incorporate volunteer during clean-up of post-hurricane disaster [4].

The spontaneous volunteers can be a significant resource. However, a mechanism to efficiently utilized the volunteers need to be designed effectively to avoid a scenario that can distract responders from delivering their duties and create problems such as security, safety and health problem to the disaster area. Efficient volunteer management systems (VMS) are widely used to efficiently utilize available volunteer resources while ensuring the safety and ability of the volunteers to perform assigned tasks. Various systematic approach to establishing requirements and manage the incidents related to specific disaster had been proposed. Technology advancement in information and communications technology enable the deployments of the VMS that contain information that can be used across the organizations such as government bodies, rescue teams, disaster management teams, military, volunteers, citizens, media

This paper provides an overview of VMS and its challenges, focusing on the process of volunteers' recruitment and management of volunteers' personal information that needed to be handled according to the information security concept which is privacy, security, accessibility and control. This paper proposed VMS design for Malaysia and review security concern which also includes concern on trust issues that may arise between government coordination agencies and the volunteers in managing sensitive information either from government agencies side or volunteers' side. The proposed VMS includes the concept of trust and the implementation of security by design concept at the development phase

Revised Manuscript Received on February 11, 2019.

Noor Afiza Mat Razali, Defence Science and Technology Faculty, National Defence University of Malaysia, Kuala Lumpur, Malaysia.

Nurjannatul Jannah Aqilah Md Saad, Defence Science and Technology Faculty, National Defence University of Malaysia, Kuala Lumpur, Malaysia.

Hasmeda Erna Che Hamid, Defence Science and Technology Faculty, National Defence University of Malaysia, Kuala Lumpur, Malaysia.

Muhammad Ramzul Abu Bakar, Defence Science and Technology Faculty, National Defence University of Malaysia, Kuala Lumpur, Malaysia.

Khairul Khalil Ishak, Center of Cyber Security and Big Data, Management and Science University, Selangor, Malaysia.

Nor Asiakin Hasbullah, Defence Science and Technology Faculty, National Defence University of Malaysia, Kuala Lumpur, Malaysia.

Norulzahrah Mohd Zainudin, Defence Science and Technology Faculty, National Defence University of Malaysia, Kuala Lumpur, Malaysia.

Suzaimah Ramli, Defence Science and Technology Faculty, National Defence University of Malaysia, Kuala Lumpur, Malaysia.

Norshahriah Wahab, Defence Science and Technology Faculty, National Defence University of Malaysia, Kuala Lumpur, Malaysia.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

II. DISASTER MANAGEMENT AND VOLUNTEERISM

When a disaster happened, a disaster relief and emergency resource will be distributed to the affected area that requires efforts, especially from the front line in providing rescue, health and medical assistance [5]. Right after a natural disaster occurred, efficient emergency logistics distribution which is the urgent relief needs must be distributed to the affected areas quickly as it is vital in alleviating the disaster impact [6]. According to [5], [7], relief supply collaboration is relatively critical in order to manage emergency logistics following the natural disaster on affected areas. Due to changes in multiple factors in a disaster situation that resulted in a higher public emergency, thus increasing demand for emergency resources. This refers to minimum guarantee requirements for an effective response which is a response to public emergencies should be efficient and emergency resource also should be used in highly efficient [8].

In Malaysia, disaster is managed by the National Disaster Management Agency (NADMA) under the Directive 20 of the National Security Council that act as the focal point in managing disaster [9] that have 3 levels of disaster management at district level, state level and national level [10], [11]. Each level consists of specific agencies that will deploy relief operation during disaster [11] as shown in Table 1. The first of disaster is described as any disaster that involves local incidents which have potential to spread will be managed by District Disaster Management and Relief Committee (DMRC). In level two, disaster will be managed by State Disaster Management and Relief Committee (SDMR) and on level three, Central Disaster Management and Relief Committee (CDMRC) are responsible in managing disaster management that includes forming a central, state and district level of disaster management [9], [10].

Table 1: Level of disaster in Malaysia

Level of Disaster	Descriptions
Level 1	Involve local incidents which have no potential to spread - Managed by District Disaster Management and Relief Committee (DDMRC)
Level 2	More serious incidents covering wide areas (2 districts) with the potential of spreading - Managed by the State Disaster Management and Relief Committee (SDMR)
Level 3	Complex in nature and affecting a wide area - Managed by the Disaster Management and Relief Committee (CDMRC)

In managing disasters, a side of high skills responsible authorities, volunteers also contribute to the rate of relief operation efficiency [2], [3]. Volunteers could complement the authorities by leveraging skills that are lacking on the scene contribute to economic saving [4], [12]. Involvement of public community and volunteers during each of disaster cycle (pre-disaster, during disaster, post-disaster) is vital. United Nations International Strategy for Disaster Reduction (UNSDR), Hyogo Framework for Action 2005 -2015 (HFA), outline a foundation of promotion, enhancement and empowerment in "adoption of policies, strategic management of volunteer resource and attribution of roles and responsibility and delegation and provision of the necessary authority and resource" [13].

A. Volunteer Registration and Approval Process

Giving the nature of disaster management that includes involvement of volunteers from different background and never worked together before, it should be noted that there are several aspects to address the security issue for VMS from a volunteer perspective. However, little attention had been paid to the security aspect of managing the identity of the volunteer. Volunteer personal information must be validated and verified. During the process of volunteer's registration to VMS, a background check is crucial and necessary to determine either the person is eligible to be a volunteer with clean background history.

There are several VMS that applied a background check as the tone of their VMS's features. As an example, eRecruiter and eCo-ordinator by Samaritan provide a mechanism of the instant background check of a volunteer with instantaneous results [14], [15]. Community Event Registration and Information System (CERVIS) also provide background checking of the new volunteer by checking either the person is eligible to be a volunteer with a clean background history [16]. Most of the VMS available is doing integration with the third party to do a background check. As an example, by having a collaboration with any agencies or organization that could provide information on the background check of their applicant. Aside from that, they can also rely on recruiting volunteers from an organization that already have a registered volunteer. Example, Volgistics let organization to handle all volunteer registrations, while The Raiser's Edge (i)™ is directly recruiting volunteers from an organization's website [17]. Background check not only to alert administration on a person's background, but it also to determine if the person is eligible to be a volunteer according to their terms and condition [18], [19]. Hence, we can see that existing VMS applied the background check as in determining only eligible volunteers can be on disaster-affected area thus helping authorities in the relief operation.

B. Volunteer Distribution Process

VMS gathers potential volunteers and optimizing and mobilizing the volunteers during specific events by scheduling, task distribution and provide a medium of communication that facilitates the coordination mechanism and collaboration between various institutions. There are emerging of free and open source software (FOSS) or paid software of VMS in having more systematically coordination and dissemination of volunteer that is said can

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

help in managing humanitarian response resource, distribution of response intelligent and coordinating response operational [20]. The most important aspect in developing VMS is to have a provision of intelligent feedback from people on the scene [21]. Technology is vital in extending human capabilities in coping with disasters that are either natural or man-made factor [22]. Therefore, information communication technology (ICT) plays an important role during the disaster, especially in enabling rapid and efficient humanitarian aid for crisis management issue [23].

III. SECURITY ISSUES IN VOLUNTEER MANAGEMENT SYSTEM

In disaster management aspects, data regarding disasters from both government and private sector collect as big data in determining disaster's risk, leveraging and in constructing emergency response operation [24]. Managing information on a large scale is a challenging task due to its diversity, dynamic behavior, geographical distribution and not to mention its large amount [24] and deal on response data quality issues where it could be inaccurate, incomplete and inconsistent [25] and thus will be resulted in security and privacy violation [26].

In merging and integrating vast data from various organizations into centralized data is a huge challenge need to face as large amount of data deal with security related issues. Storage, management and analytics of big data tightly link to security and privacy issues by centralizing all data into one pool, the risk of getting attack is higher as data are becoming more valuable to an attacker and indirectly it will leave huge wrath on information exposed. Exposure of information will lead to issues of trust by organizing towards the data collector [27], [28]. Hereby, making a proper controlled and protected big data stores are indeed crucial [22], [27]. On the other hand, in [24] also addressed that limitation on communication approach, especially on the Internet is also a merging issue in maintaining VMS functionality. Network under crisis is most likely is in manners of chaotic overload, reliability and in security aspects [29]. Network disconnection will result in data loss and thus miscommunication will happen [24] and thus make it undeniably critical in making a timely decision during disaster [30].

Volunteers came from various backgrounds and perhaps will meet for the first time when the disaster occurred, and they are assigned to the same scene. Researchers proposed that there are 3 context of trust that directly related to VMS development. 1) Trust within an organization, basically on trust development among workers under an organization, 2) trust between different organization where revolve on building trust between each worker form a different organization and 3) trust among organization and their customer [19]. Researchers also are proposing that inter-organizational trust consists of 4 types of trust, - 1) trust based on goodwill and how much of a person considering other to be a friend judgmental, 2) trust based on perceived ability on how others can carry out task well, 3) trust based on behavioral either the attitude is contractual to the agreement and 4) trust based on the expediency of need to carry out task to meet the desired goal or outcome quickly [31].

Other than that, in defending and preventing the system from any attack, most developers enhance system security by extending system design pattern by applying the specific security functionality by implementing security components such as access control, authentication, and authorization (AAA). Extended security design with specific security functionality can lessen risk and probability of the system being attacked. The security design concept is divided into 3 which is (1) Architectural-level patterns, (2) Design-level patterns and (3) Implementation-level patterns [32]. In architectural-level patterns, privilege separation and user role are what it focused on. As an example, in PrivSep (Privilege Separation), the user is divided their authorization and authentication on system functionality based on their privilege. For design-level patterns, it involves data management in the database and secure coding method. As an example, in a database, admin can view all user information, but not applicable for another user. It is related to the use of persistent data management system (PDMS). As for implementation-level patterns, it is focusing on system log and sensitive information. Table 2 shows all functions available in all three patterns [32].

Table 2: Security function in security design conceptualization

Security Design Level	Security Functions
Architectural-level pattern	1. Distrustful Decomposition 2. PrivSep (Privilege Separation) 3. Defer to the Kernel
Design-level pattern	1. Secure factory 2. Secure Strategy Factory 3. Secure Builder Factory 4. Secure Chain of Responsibility
Implementation-level pattern	1. Secure logger 2. Clear, sensitive information 3. Secure directory 4. Input Validation 5. Pathname Canonicalization

IV. RESULTS & DISCUSSIONS

For smooth deployment of volunteers, locality factor needs to be emphasized. We propose that VMS design as shown in Fig. 1 and Fig. 2, so that it matches locality of the supporting environment. Fig. 1 shows the flowchart of the volunteer registration process and Fig. 2 shows volunteer request by admin. In VMS, there are 3 main users-admin, volunteer manager and volunteer. Hence, the concept of least-privilege on each user role is crucial to maintaining data protection and security. This concept is restricting the user from accessing data based on the authorization's level. As an example: Admin can access all data of users with but admin can't change any data or information about manager and volunteer unless the admin is told to do so. Through this, input data by manager

and volunteer are kept secure and unchanged. CIA triad must be followed during the development of VMS. Table 3 shows an example of a user role based on CIA triad. On the other hand, VMS's entity role is described in use-case as shown in the figure below. Fig. 3 shows the role of admin in VMS including managing other entity's activity in VMS. Admin and Manager are most likely having a similar role in term of managing volunteer. But, the admin's role is more crucial in managing all entity's information data. As for manager in Fig. 4, it only manages volunteers' activity by requesting and monitor volunteers task completion during a disaster.

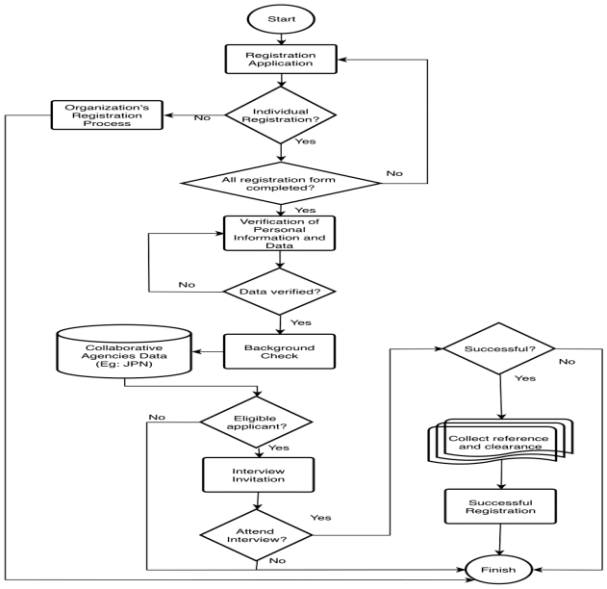

Fig. 1:Example flowchart process volunteer request by admin

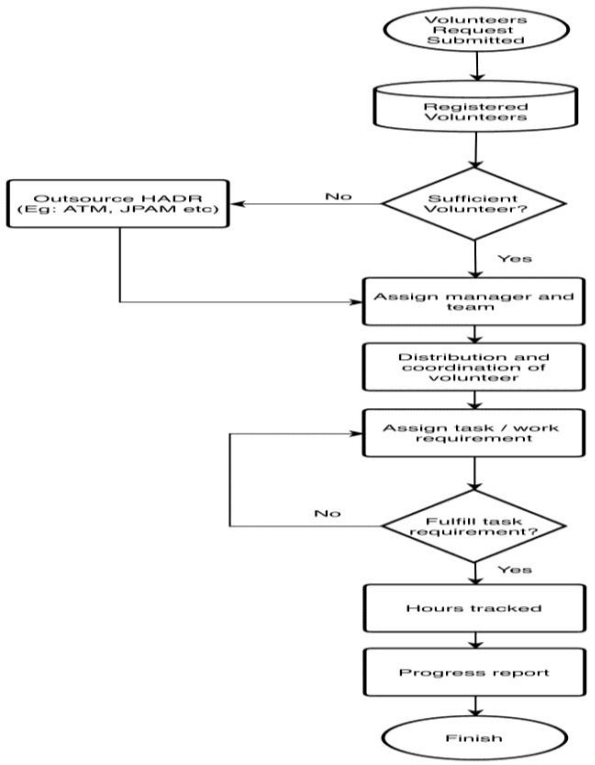

Fig. 2:Example flowchart process volunteer request by admin

Table 3: Security function in security design concept

CIA Triad	User Role
1. Confidentiality	
1.1 Admin	Access on all user's profile but cannot edit the data
1.2 Manager	Access and editing on manager's profile only
1.3 Volunteer	Access and editing on volunteer's profile only
2. Integrity	
2.1 Admin	Manage and authorized manager's and volunteer's schedule reports and tracking
2.2 Manager	Can only view manager's profile data and information on the certain field of content only (volunteer work list, schedule) – manager ID can't be edited or deleted
2.3 Volunteer	Can only view volunteer's profile data and information on the certain field of content only – volunteer ID, work list and schedule of the project can't be edited or deleted
3. Availability	
3.1 Admin	Access of database of all users – schedule, personal information, tracking and report, expenses etc.
3.2 Manager	Manage and edit volunteers' list of criteria/work to do and view volunteer's report
3.3 Volunteer	View and execute a list of criteria/work to do by the manager

Manager act as the middle-user that connects volunteer to admin through operation executed on volunteer. Fig. 5 shows volunteer role in data entry during the volunteers' registration.

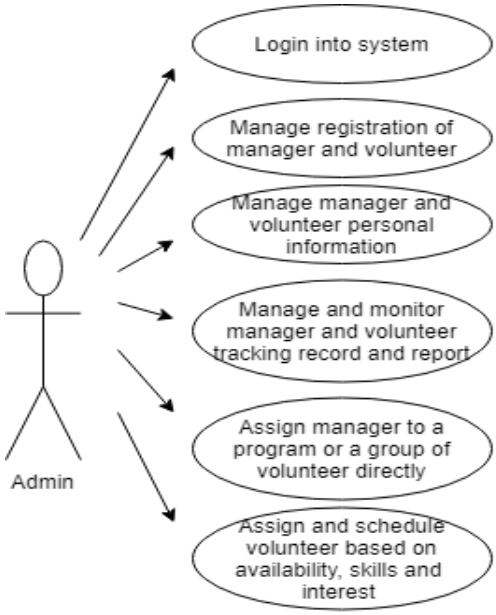

Fig. 3: Proposed admin role in VMS

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

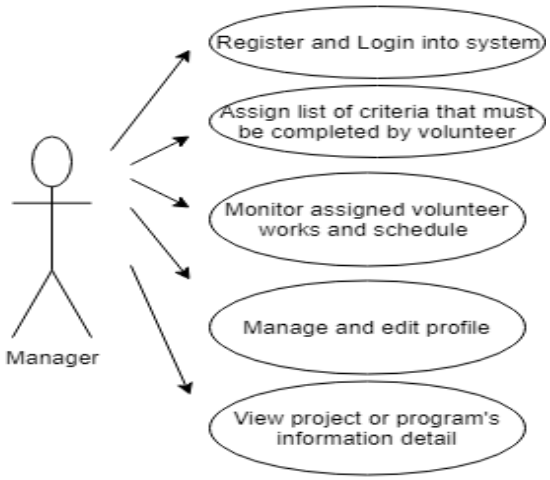

Fig. 4: Proposed manager role in VMS

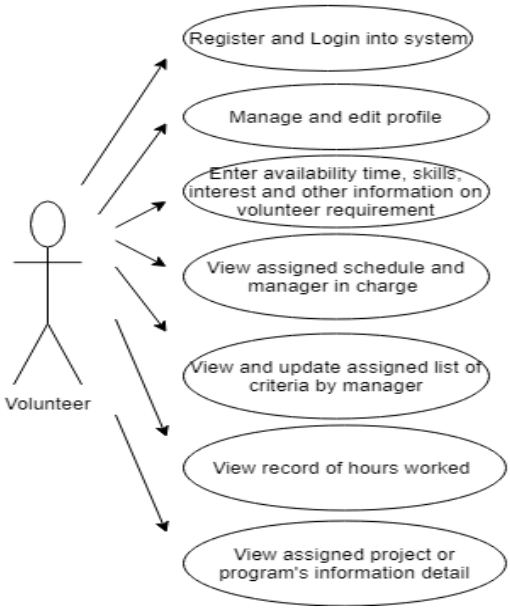

Fig. 5:Proposed volunteer role in VMS

Hence, in the development phase, the connection between actors in VMS bring up trust issue specifically in data management. This study is discussing trust within the organization as the main subject to be included in a trust mechanism while designing VMS by emphasizing of implementing an element of trust in the VMS design.

Table 4: Trust issues model in VMS

Trust Type	Issues on VMS Based on Volunteer Perspective
Trust 1: Personal Trust	How well volunteer will put their trust in other volunteers to carry out any task assigned
Trust 2: Managing Trust	How well can manager/administrator put their trust in volunteers in perceiving good attitude while carrying out the task to keep a safe environment on the community they served.
Trust 3: Data Trust	How well volunteer can put trust in the administration of VMS to handle and manage their personal information

Table 4 shows the summary of our proposal on trust type that should be addressed while designing VMS. Design of VMS should take trust as consideration while building the VMS for a particular organization by implementing the concept of security by design concepts.

A. Security and Trust Framework for VMS

In developing a secure VMS in the aspect of information security, security by design concept need to be implemented. Fig. 6 shows propose overview security characteristic of VMS development flow and requirement. In this design, we inject the concept of security of design in developing VMS aside considering the human factor (trust issue).

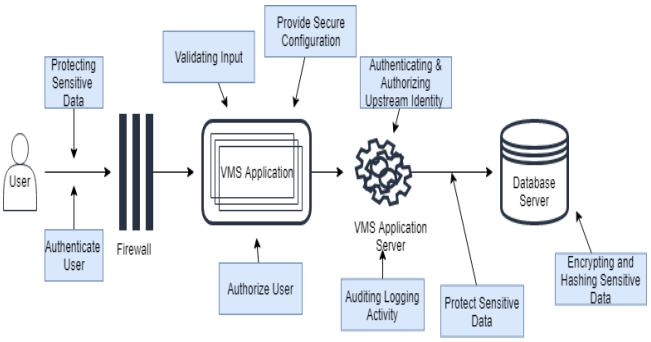

Fig. 6:Proposed required characteristic in developing VMS

Table 5 shows the proposed security function that can be implemented during the system development life cycle for the time being based on a literature review.

Table 5: Proposed implementation of security function by design in VMS

Security Design Level	Security Functions
Architectural-level pattern	1. Distrustful Decomposition 2. PrivSep (Privilege Separation)
Design-level pattern	1. Secure factory 2. Secure Strategy Factory 3. Secure Chain of Responsibility 4. Secure State
Implementation-level pattern	1. Secure logger 2. Input Validation

In Architectural-level patterns, Distrustful Decomposition is where system have different and separate programs for each process with a unique ID that do not have any privilege or sharing with other ID. It basically differentiates programs for each logged user. PrivSep (Privilege Separation) is focusing on the authentication process which is pre-authentication and post-authentication. As an example, in VMS, a volunteer who wishes to register and logged as authenticate user on VMS, they need to wait for system authentication approval before accessing other function available for logged volunteers. In Design-level patterns, Secure Factory concerns on constructing different versions of programs or object based on users' credentials. Secure Factory is related to Secure Factory Builder and Secure

Chain of Responsibility that involved in separating the design of a system based on users' credentials. At this part, only authenticated and authorized user can view existing functions. All this function related to data stored in a database on identifying authorized user where selected security credential will return an appropriate object based on security credential.

As an example, logged admin can only view the admin function interface, the logged manager can only view manager function interface and logged volunteers can only view volunteer interface function. This led to a Secure State implementation where defines interface representing each user that handle by operation handler. Fig. 7 shows an example of data retrieval and view based on user credential and Fig. 8 shows example of Secure State of VMS. In Secure State, default user will be shown the same interface. In VMS, all user will be directed to VMS main page and then login interface if they want to view high privilege function. And when users logged in with respected credentials, they will be directed to their respected function interface based on their credentials.

In Implementation-level patterns, Secure Logger is what we need to apply strongly. This function prevents the system from being modified by the attacker through edited system logger. This can be achieved by a secure logger. Input Validation will be used in determining the type of data inserted in preventing any attack such as SQL injection, cross-site scripting attack and buffer overflow attack.

Input Validation can be done by defining criteria for data such as Numerical Data ( ) and String Data ( ) which use in HTTP form for GET and POST parameter. Aside from that, the code function in handling invalid data entered by the user also will be implemented. As an example, in the registration form, volunteers can only insert numerical data ( ) in IC/Passport field.

In developing a secure VMS in the aspect of information security, trust issue of entities needs to be addressed as it complies with the security of a system. Fig. 9 shows trust issues among entities. From the volunteer's perspective, their personal information is what they concerned when registered in a VMS on how it will be handled, managed and used by the authorities. Personal information security falls under the aspects of information security. Hence, in this matter, volunteers will have some trust issue on authorities that managed their information on VMS. Hence, this strongly suggested that the concept of security by design of a system should be emphasized in preserving user's personal information in the aspect of security and privacy. Fig. 10 presents our proposed framework of trust attribute in VMS design. Personal Trust (T1) - is portrayed by volunteer on how well volunteer can trust another volunteer in carrying out assigned task/job.

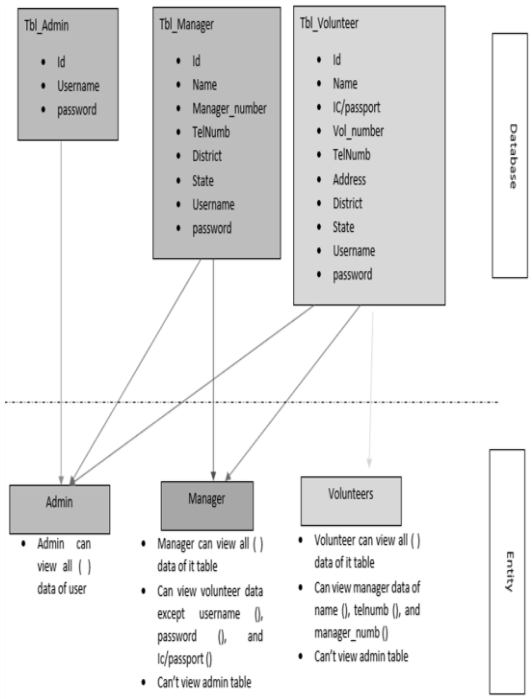

Fig. 7: Example of data retrieval and view based on user credential

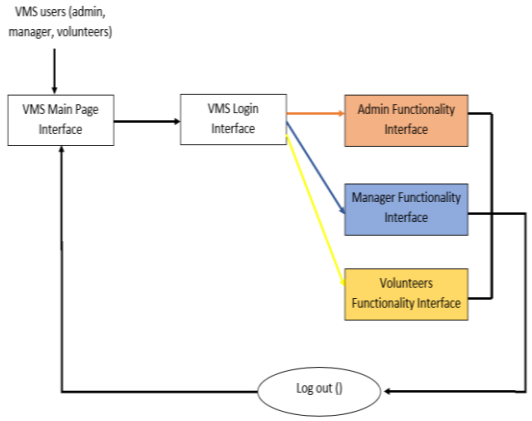

Fig. 8: Example of secure state of VMS

Managing Trust (T2) are related to each entity – volunteer and Admin. Safety of volunteer –volunteer need to trust in admin to keep their safety during carrying out task/job. As for Data Trust (T3), volunteer needs to trust admin on keeping privacy and safety of their information by not selling their data to any organization and just for VMS storage.

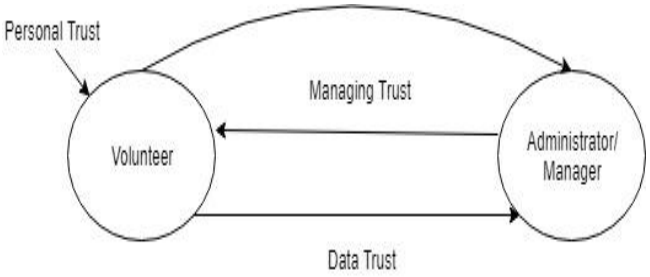

Fig. 9: Relation of trust in VMS

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

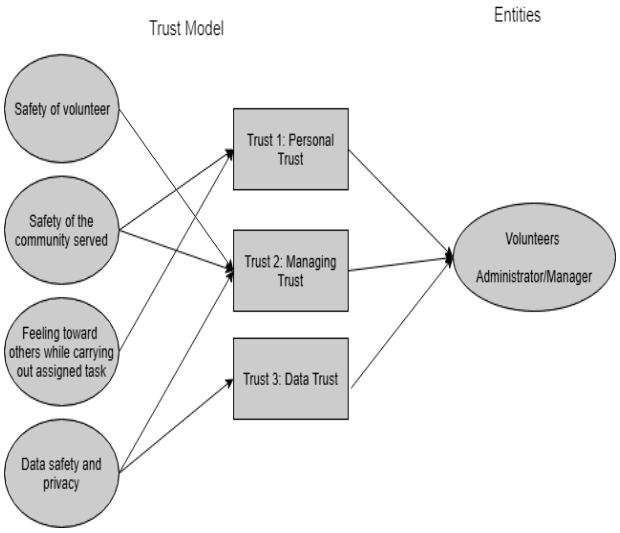

Fig. 10: Relation of trust in VMS on entities

V. CONCLUSION

VMS must be designed by considering the information security triad and implement the security by design concept. Security requirement needs to be emphasized since the early development phase aside enhancing the security of information by tackling human emotion factor as well. VMS also should be designed by considering the local coordination process and the related requirement to effectively deploy volunteer resources during a disaster. The concept of the framework presented in this paper consist of information security triad and element of trust between the entity in VMS from a volunteer perspective. Low levels of interpersonal trust among individuals in society may result in a desire for more government involvement to protect personal information privacy and security. As future work, the prototype for VMS using the proposed framework will be developed. Validation of the security components and trust issues proposed in this study will be validated with target subjects which are volunteers and authorities who manage VMS in Malaysia.

REFERENCES

1. I. M. Shaluf and F. Ahmadun, "Disaster types in Malaysia: An overview," Disaster Prev. Manag. An Int. J., 15(2), 2006, pp. 286–298.
2. F. Wex, G. Schryen, S. Feuerriegel, and D. Neumann, "Emergency response in natural disaster management: Allocation and scheduling of rescue units," Eur. J. Oper. Res., 235(3), 2014, pp. 697–708.
3. J. Whittaker, B. McLennan, and J. Handmer, "A review of informal volunteerism in emergencies and disasters: Definition, opportunities and challenges," Int. J. Disaster Risk Reduct., 13, 2015, pp. 358–368.
4. L. S. Fernandez, J. A. Barbera, J. R. Van Dorp, F. Lauren, J. A. Barbera, and J. Van Dorp, "Strategies for managing volunteers during incident response: A systems approach," Homel. Secur. Aff., 2(3), 2006, pp. 1–15.
5. L. E. De la Torre, I. S. Dolinskaya, and K. R. Smilowitz, "Disaster relief routing: Integrating research and practice," Socioecon. Plann. Sci., 46(1), 2012, pp. 88–97.
6. J. B. Sheu and C. Pan, "Relief supply collaboration for emergency logistics responses to large-scale disasters," Transp. A Transp. Sci., 11(3), 2015, pp. 210–242.
7. S. Roh, A. Beresford, and S. Pettit, "Challenges in humanitarian logistics management: An empirical study on pre-positioned warehouses," 20th Int. Symp. Logist., 2015, pp. 1-8.
8. W. Liu, G. Hu, and J. Li, "Emergency resources demand prediction using case-based reasoning," Saf. Sci., 50(3), 2012, pp. 530–534.
9. Center for Excellence in Disaster Management and Humanitarian Assistance. Malaysia: Disaster management reference handbook. 2016, Available: https://reliefweb.int/sites/reliefweb.int/files/resources/disaster-mgmt-ref-hdbk-Malaysia.pdf.pdf.
10. S. Shafiai and M. S. Khalid, "Flood disaster management in Malaysia: A review of issues of flood disaster relief during and post-disaster," European Proceedings of Social and Behavioural Sciences, 2016, pp. 163–170.
11. A. W. Suhaimi, N. A. Marzuki, and C. S. Mustaffa, "The relationship between emotional intelligence and interpersonal communication skills in disaster management context: A proposed framework," Procedia - Soc. Behav. Sci., 155, 2014, pp. 110–114.
12. T. R. Johnson, Disaster volunteerism. 2014, Available: http://aboutiigr.org/wp-content/uploads/2015/01/Disaster-Volunteerism.pdf.
13. International Strategy for Disaster Reduction, Hyogo framework for action 2005-2015. 2005, Available: https://www.unisdr.org/2005/wcdr/intergover/official-doc/L-docs/Hyogo-framework-for-action-english.pdf.
14. K. Andrei, C. Bernard, J. Leslie, and L. Quinn, A consumers guide to software for volunteer management. 2011, Available: https://www.techsoup.org/SiteCollectionDocuments/article-consumers-guide-to-software-volunteer-management-document.pdf.
15. J. Schonbock, M. Raab, J. Altmann, E. Kapsammer, A. Kusel, B. Proll, W. Retschitzegger, and W. Schwinger "A survey on volunteer management systems," IEEE 49th Hawaii Int. Conf. Syst. Sci., 2016, pp. 767–776.
16. D. Ceresoli, QE-GIPAW user's manual. 2012, Available: https://github.com/dceresoli/qe-gipaw/blob/master/doc/user-manual.pdf.
17. M. A. Hager and J. L. Brudney, Volunteer management: Practices and retention of volunteers. 2004, Available: https://www.urban.org/sites/default/files/publication/58001/411005-Volunteer-Management-Practices-and-Retention-of-Volunteers.PDF.
18. National Health Service England, Recruiting and managing volunteers in NHS providers: A practical guide. 2017, Available: https://www.england.nhs.uk/wp-content/uploads/2017/10/recruiting-managing-volunteers-nhs-providers-practical-guide.pdf.
19. K. K. Ishak, N. Afiza, M. Razali, A. M. Lokman, and K. Toshiyuki, "Kansei information security assessment (KISA): Characterizing trust as stimuli for user emotional assessment in information security," Indian J. Sci. Technol., 9, 2016, pp. 1–6.
20. R. Morelli, C. de Silva, T. de Lanerolle, R. Curzon, and X. S. Mao, "A global collaboration to deploy help to China," Commun. ACM, 53(12), 2010, pp. 142-149.
21. L. Carver and M. Turoff, "Human-computer interaction: The human and computer as a team in emergency management information systems," Commun. ACM, 50(3), 2007, pp. 33–38.
22. I. J. Sinthiya and E. Shanmugapriya, "Big data in disaster management," Engineering and Technology in India, 1, 2016, pp. 86–108.
23. C. B. Nelson, B. D. Steckler, and J. A. Stamberger, "The evolution of hastily formed networks for disaster response: Technologies, case studies, and future trends," IEEE Glob. Humanit. Technol. Conf., 2011, pp. 467–475,.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

24. J. Li, Q. Li, C. Liu, S. Ullah Khan, and N. Ghani, "Community-based collaborative information system for emergency management," Computers and Operations Research, 42, 2014, pp. 116–124.
25. J. P. Li, R. Chen, J. Lee, and H. R. Rao, "A case study of private-public collaboration for humanitarian free and open source disaster management software deployment," Decis. Support Syst., 55(1), 2013, pp. 1–11.
26. B. Thuraisingham, "Big data security and privacy," 5th ACM Conference on Data and Application Security and Privacy, 2015, pp. 279–280.
27. C. Tankard, "Big data security," Netw. Secur., 2012(7), 2012, pp. 5–8.
28. S. Kaisler, F. Armour, J. A. Espinosa, and W. Money, "Big data: Issues and challenges moving forward," 46th Hawaii Int. Conf. Syst. Sci., 2013, pp. 995–1004.
29. T. Bui, "A framework for designing a global information network for multinational humanitarian assistance / disaster relief," Network, 1(4), 2000, pp. 427–442.
30. W. L. Waugh and G. Straib, "Collaboration and leadership for effective emergency management," Public Adm. Rev., 66(suppl. 1), 2006, pp. 131–140.
31. G. Dietz and D. N. Den Hartog, "Measuring trust inside organisations," Pers. Rev., 35(5), 2006, pp. 557–588.
32. C. Dougherty, K. Sayre, R. C. Seacord, D. Svoboda, and K. Togashi, Secure Design Patterns. 2009, Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a636498.pdf.