International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Multi-Cast Policy Management Process for Improved Network Security with the Group-Oriented Applications

Nanang Yusroni*[1] , Dhruv Galgotia[2] , Aniruddha Bodhankar[3] , Hendy Tannady[4] , H.Mary Henrietta[5] , Mr. Akash Kumar Bhaga[6]

Submitted: 18/08/2022 **Accepted:** 25/11/2022

Abstract: The increased Internet utilization leads to emerging group-basedapplications such as military, healthcare, online collaboration, video conferencing and so. However, in the group-oriented application resources are secured through a constraint network. The promising multi-cast communication group-oriented communication model exhibits reduced bandwidth with the different decentralized group key management such as the decentralized group key framework. In this paper, proposed a Multicast Polynomial Key Distribution Scheme (MPKD)model with acentralized and decentralized key management framework. The proposed MPKD model comprises of the three process such as generation of key, distribution of key and refreshment of key. The proposed MPKD mode uses the logical key tree structure with the computation of the polynomial in the key generation process. The performance analysis is based on the structure protocol with the key distribution in the centralized framework model. The performance of the proposed MPKD model is comparatively examined with the conventional OFT, SKD and MUKD model. The analysis of the results expressed that proposed model ~2% - 4% reduces the communication and storage cost. The storage cost of the existing model exhibits the value of maximal 63 but the proposed MPKD model achieves 34 for the user count of 32. Similarly, the communication and storage cost is minimal for the unicast and multicast communication.

Keywords: *Group-oriented communication, Multi-cast policy, Policy management, polynomial, Communication cost, Storage Cost*

1. Introduction

In recent years, Internet-based group-based application exhibits significant advancement in the home, char, video conferencing, healthcare, military and so on [1]. The increase in the group communication focused on the security with the resource constraint network. The secure group communication is a communication between group of members where all the members are interconnected and all are able to communicate with each other in a secure manner [2]. At the same time, each member is securely isolated from all others. When the confidential data or commercial value data are transmitted in a group, it is mandatory to protect the group communication from the unauthorized access through suitable security mechanisms [3].Before proceeding further, it is necessary to clarify the reason for choosing the appropriate communication model for the secure communication. The applications like video on demand and video conferencing force the transmission of multimedia data in the group communication [4]. The bandwidth requirement of the multimedia transmission is higher than the ordinary data communication. When the security mechanisms are incorporated in this situation, the efficiency of the group communication is affected [5]. This reveals that the secure group communication in a resource constraint environment is not only compelled by the security mechanisms but also striving by the communication content [6 – 9]. Hence, it is mandatory to choose an appropriate efficient communication model without compromising the security of the group communication. The group communication can be carried out in the following ways namely [10]: Unicast, Multicast, Broadcast and Anycast. The security issues of group communication are discussed. IP multicast is an open structure and does not provide any support for closed group, because the multicast address is publicly available to all [11]. Due to the open structure, any node can easily join in the group without getting any permission from the network router. This simplicity leads to a lot of security challenges and vulnerabilities. Denial of Service: Implementing access control is very difficult in the multicast group communication, because the receiver does not have any provision to send their interest directly to receive the group message to the source. Eavesdrop: Since no access control is involved in multicast group communication [12], the data transmission is carried out through unsecure channels. Hence, eavesdropping opportunities are higher in the group communication.Masquerade: In the group communication using IP multicast, there is no mechanism to check the identity of the sender of the group message. So any non-legitimate member can join in a group and act as a valid member and can involve in the group communication.Leakage of Information: If there is a

[1]*Universitas Wahid Hasyim, AccountingFaculty of Economy Semarang nanangyusroni@unwahas.ac.id*
[2] *Professor, Department of Management, Galgotias University, Greater Noida, Uttar Pradesh,India, ceo@galgotiasuniversity.edu.in,*
[3] *Department Management, Assistant Professor, Dr.Ambedkar Institute of Management Studies & Research,Nagpur aniruddha.bodhankar16@gmail.com*
[4] *Universitas Multimedia Nusantara, Management College name: Faculty of Business, Tangerang hendy.tannady@umn.ac.id*
[5] *Assistant Professor(SG, Department of Mathematics, Saveetha Engineering College(Autonomous), Chennai, mary.henriet123@gmail.com*
[6] *Assistant Professor, School of Engg.&IT ARKA JAIN University, Jamshedpur, Jharkhand, India akash.b@arkajainuniversity.ac.in*

possibility of having masquerader in the group, then information leakage may occur [13]. Hence, the unauthorized member of the group can read the group message and may involve in illegitimate activities.

2. Related Works

With the decentralized key management scheme, the multicast members are fragmentedinto different smaller subgroups that are controlled by a variety of groups [13]. However, the scenario is the elimination of the vulnerability in the single point with the effect of N issues with the reducing the cost of the key. The review is based on the examination of the decentralized key management scheme for group-oriented communication. In [14] proposed various evaluation metrics to carry out the performance analysis in terms of efficiency and security. The efficiency of the investigated protocols can be analyzed in terms of cost of communication, storage and computation. The security analysis expressed that the secrecy is effective for forwarding, backward and group key.

In [15] proposed the use of Logical Key Hierarchy. In this protocol, all the keys are logically mapped into tree structure. In this tree structure, all leaf nodes correspond to the group members and each member has the keys of the nodes that lies on the path from leaf to root node in the tree. Hence, every member holds log 2 n+1 keys. The non-leaf nodes correspond to the group managers which possess Key Encryption Keys (KEK) and the root is the server that possesses Traffic Encryption Key (TEK) or group key. Whenever a node joins in a group, all the keys that lies on the path from the new member to root must be changed. The server creates a new TEK and new KEKs of the intermediate nodes which are on the path of root to leaf and individual key of the new member. In [16] proposed a One-way Function Tree (OFT) for the improvement of LKH. The OFT model uses the binary tree for the key management implementation in bottom-up approach. The process of key refreshment and generation is performed from the tree bottom.

3. Proposed Multicast Polynomial Key Distribution Scheme (MPKD)

The proposed MPKD mode uses the logical key structure for the generation of the multicast key in the group-oriented communication. The proposed model comprises of the members (N) are places in the tree leaf nodes. The members in the higher level of SMs are located in the Heads of the SMs (HSM) are in the higher level. Between the members the maximum hop count is estimated as the SM in the one key tree. Each member in the tress generate the secret key and shared to the subgroup manager with the unicast scenario as shown in figure 1. The shared secret keys comprise of the Diffie-Hellman exchange for the key management. The embedded key is evaluated with the polynomial expression those are distributed between the groups with the multicase approach. For every subgroup the manager is responsible for the process of key management with the inter-group HSM assists key distribution in the subgroups. The subgroup manager is involved in the management of key and intergroup communication assistance. The root node is responsible for the authentication and prevention of attacks.

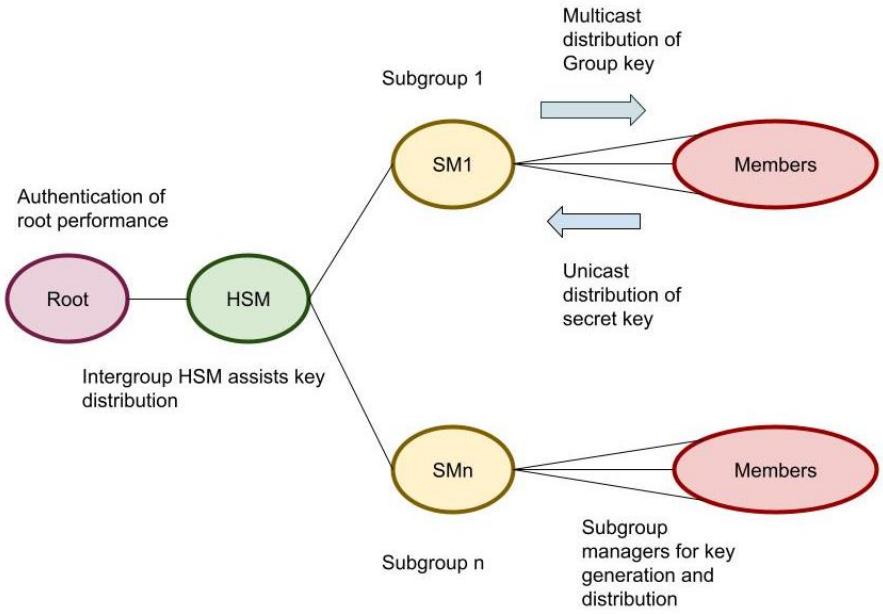

Figure 1: Key distribution in MPKD

The process flow diagram of MPKD is shown figure 2. Like MUKD, MPKD also starts with subgroup formation. The nodes having hop count one with others can form a subgroup. After subgroup formation, the manager for each subgroup is elected. To elect the Subgroup Manager, each member shares its MAC value to all other members. The highest weighing node is selected as the manager of that subgroup. The other members register with the SM to become the authorized members of that subgroup. After registration, each member securely shares its Secret Key to the SM using unicast approach. The SM generates the group key using Diffie- Hellman key exchange algorithm. Again the SM generates a polynomial based on the generated group key and the SKs. Then, SM multicast the expanded polynomial without encryption to all its members. When the authorized member receives the polynomial, the member easily derives the group key by substituting the SK. Through the polynomial unauthorized members the group keys are not derived. Additionally, with the factorization of the polynomial in MPKD it is difficult to perform.

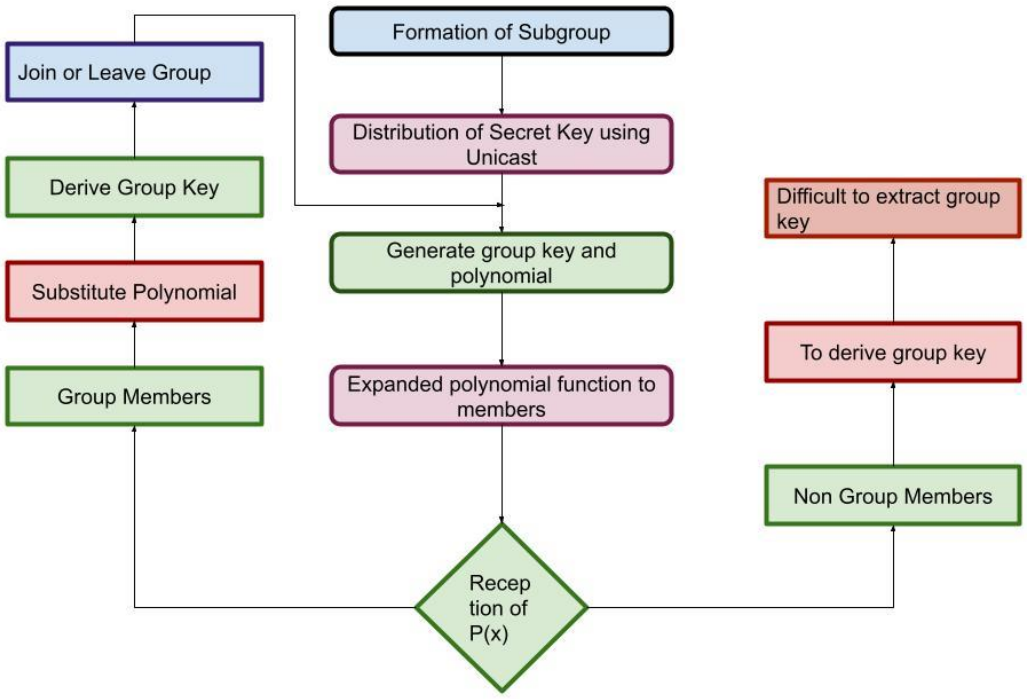

Figure 2: Flow Chart of MPKD

Consider the subgroup as S, subgroup mangers as SM and N members are involved in SM. Every member in the SM tend to ranges from Ni (i=1 to n) involved in the transmission of information from SK_i to SM. The process of SM uses the Diffie Hellman key exchange for the generation of the common key group.

The generated keys are defined as the (N_i *as the members*, SM as subgroup manager, Secret Keys SK_i, Intra-Group key GK.

{

$N_i$tranmit data from$SK_i$to SM

SM elect the prime number p

SM chooses α, α is the primitive root of p and α < p

SM compute the public key$bsk_i = \propto^{ski} \ mod \ p$

SM compute the Intra-Group key $GK = \ (bSKi)^{ski} mod \ p$

}

3.1 Inter-group key generation

With the group key distribution process the manager of subgroup generates the polynomial $P(x) = \ e^{\log(x)}$ with the embedded group key. With the distributed group key process the polynomial generated by the manager is represented as $P(x) = \ e^{\log(x)}$and the embedded polynomical in the group key are expanded with the conventional encryption process. With the receiver polynomial , the derived group leys are evaluated with the secret key. In the MPKD process the key distribution is represented as SK_i, the generated polynomial of the key is represented as in equation (1)

$P(x) = \ e^{\log((l-sk_1)(l-sk_2)(l-sk_3)\ldots\ldots\ldots(l-sk_n)+GK)}$(1)

Then it is expanded as in equation (2)

$P(x) = \ e^{log l_n - l_{n-1} + l_{n-2} \ldots\ldots\ldots \pm z}$(2)

Through multicast addressing the expanded polynomial distribution function in the members are represented as the multiplied polomial those are substituted in the SK values for the derived group key presented in the equation (3) – (5)

$\rightarrow e^{logL^n - L^{n-1} + L^{n-2} \ldots\ldots\ldots \pm z}$ (3)

$\rightarrow L^n - L^{n-1} + L^{n-2} \ldots\ldots\ldots \pm z$ (4)

$\rightarrow GK \ where \ x = \ SK_i$ (5)

The key distribution process is based on the (N_i members, SM as the subgroup manager, Secret Keys SK_i, Intra-Group Key GK)

{

$N_i$transmits theSK_i to SM

SM records the value of SK_i in its table

SM generate the polynomial based on GK computed as in equation (6)

$P(x) = \ e^{\log((l-sk_1)(l-sk_2)(l-sk_3)\ldots\ldots\ldots(l-sk_n)+GK)}$ (6)

SM multicast $P(x)$to N_i

N_i receives $P(x)$and computes

N_i substitute $x = \ SK_i$ on $P(x)$

$N_i$derives GK.

}

The polynomial computed for the multicast routing is presented in equation (7)

$P(x) = \ e \log x^5 - 15x^4 + 85x^3 - 225x^2 + 274x - 114$(7)

The values are derived from the SK value assignment as (SK=1) for the polynomial derivate presented in the group key between the equation using the (8) – (10)

$\rightarrow e \log x^5 - 15x^4 + 85x^3 - 225x^2 + 274x - 114$ (8)

$\rightarrow x^5 - 15x^4 + 85x^3 - 225x^2 + 274x - 114$ (9)

$\rightarrow 1 - 15 + 85 - 225 + 274 - 114$ (10)

$\rightarrow 6$

For second member (SK=2) in equation (9) computed as

$\rightarrow 2^5 - 15(2)^4 + 85(2)^3 - 225(2)^2 + 274(2) - 114$

$\rightarrow 32 - 240 + 680 - 900 + 548 - 114$

$\rightarrow 6$

Based on the derived subgroup members the group keys are generated. The algorithm for the proposed MPKD is presented as follows:

Algorithm 1: MPKD for the group -oriented security

Procedure join (Ni is the number of members in the group, SMi denotes the subgroup manager, root Kr, Secret Keys SKi, Intra-Group Key GK)
{
Ni transmits the transmission request + SKi to SMi
SMi sends Ni request to Kr
Kr verifies for authentication
If (Mi = valid)
Sends yes to SMi
Else
rejects the request
then
if (SMi receives acceptance)
SMi records the new SKi in routing table
{
SMi generates GK' and polynomial
SMi multicast P'(x) to Ni
Ni receives P'(x) and applies x=SKi on P'(x)
Ni derives GK'
}
Else
return null.
}

4. Performance Analysis

The performance of proposed MPKD model is comparatively examined with the existing techniques those uses the OFT and SKD. The developed MPKD model is evaluated for the varying number of users maximum of 32 members. The efficiency of the proposed MPKD model for the intra-group and inter-group communication is evaluated. The effective of the proposed MPKD model is comparatively examined with the existing technique in terms of cost effectiveness key distribution function such as storage, computation and communication cost.

4.1 Communication Cost

The number of keys transmitted in the key management process is defined as thecommunciation cost. In table the estimated communication cost for the proposed MPKD model with the existing OFT, SKD and MUKD is presented. The estimated communication cost expressed that 2^5 members for the join and leave operation.

Table 1: Comparison of Key Size

	Number of message / key exchanges		
	Unicast	**Multicast**	**Multicast**
OFT	logd(n)+1	logd(n)+1	logd(n)+1
SKD	logd(n)+1	logd(n)+1	(d-1) logd(n)+1
MUKD	1	1	1
MPKD	1	1	1
MPKD (Inter Group)	2	2	2

In table 2 comparative analysis of the communication cost for the unicast and multicast scenario is presented. The figure 3 – 5 provides the illustration of the communication cost measured for the varying number of users under unicast and multicast environment is presented.

Table 2: Comparison of Communication Cost

No of User	**OFT**	**SKD**	**MUKD**	**MPKD**	**MPKD (IG)**
Communication Cost – Unicast					
2	2	2	1	1	2
4	3	2	1	1	2
8	4	3	1	1	2
16	5	3	1	1	2
32	6	4	1	1	2
Communication Cost – Multicast					
2	2	2	1	1	2
4	3	2	1	1	2
8	4	3	1	1	2
16	5	3	1	1	2
32	6	4	1	1	2
Communication Cost - Multicast					
2	2	6	1	1	2
4	3	6	1	1	2
8	4	9	1	1	2
16	5	9	1	1	2
32	6	12	1	1	2

The comparative analysis expressed that the OFT exhibits the low performance due to balanced binary tree structure. The communication cost for the SKD is observed as higher value due to the intermediate nodes in the SKD. This implies that the communication cost performance is based on the number of users.

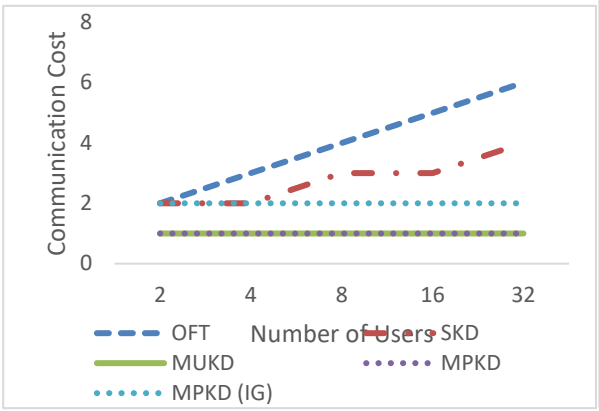

Figure 3: Comparison of Unicast

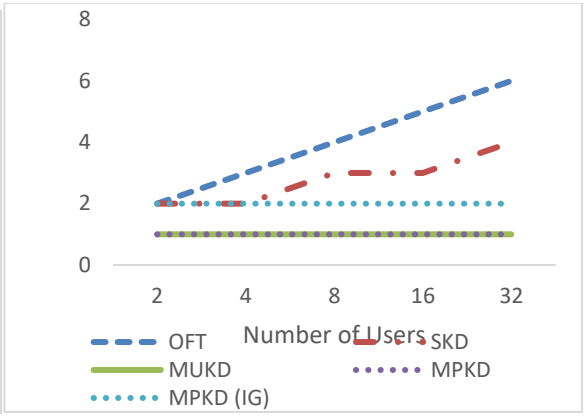

Figure 4: Comparison of Multicast

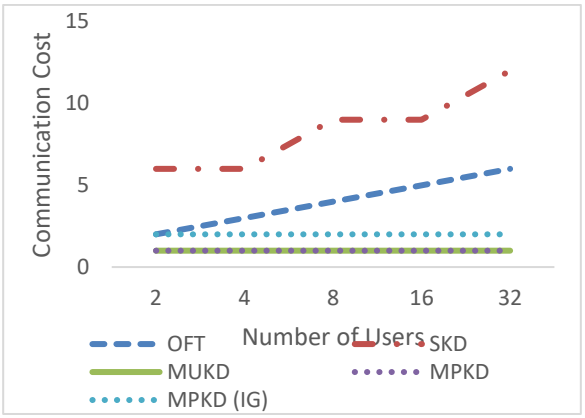

Figure 5: Comparison of MPKD (IG)

4.2 Storage Cost

In table 3 the comparative examination of the storage cost for the proposed MPKD model with the existing OFT, SKD and MUKD model is presented. The examination is based on the consideration of the 25 server members. The figure 6 and 7 provides the storage cost for the proposed MPKD model inform the Unicast and MultiCast environment is presented.

Table 3: Comparison of Storage Cost

No of User	OFT	SKD	MUKD	MPKD	MPKD (IG)
Communication Cost – Unicast					
2	3	2	3	3	4
4	7	5	5	5	6
8	15	10	9	9	10
16	31	21	17	17	18
32	63	42	33	33	34
Communication Cost – Multicast					
2	2	2	2	2	2
4	3	2	2	2	2
8	4	3	2	2	2
16	5	3	2	2	2
32	6	4	2	2	2

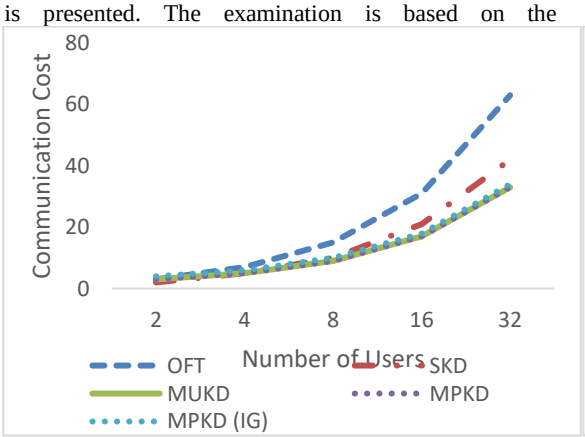

Figure 6: Unicast Storage Cost

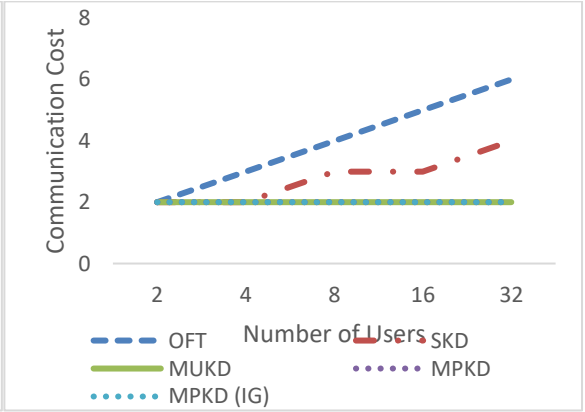

Figure 7: Multicast Storage Cost

The figure 6 and 7 expressed that the OFT subjected to the higher cost due to number of keys in the server as 2n-1. The SKD storage cost is higher and the proposed MPKD model exhibits the reduced storage cost.

5. Conclusion

With the evolution of the Internet Group-oriented communication are evolved effectively. To provides the secure communication between the group-variable MPKD based muticast scheme is developed. The proposed MPKD model uses the tree architecture for the analysis of the key in the variables. The proposed model is evaluated for the Unicast and Multicast environment for the group-oriented communication. The comparative analysis expressed that the proposed MPKD model exhibits the improved efficiency for the unicast and multicast environment. The proposed MPKD model achieves the minimal communication and storage cost compared with theexisting OFT, SKD and MUKD model. The proposed model achieves the storage cost of 34 which is significantly minimal than the existing model. The proposed MPKD model achieves the ~2% - 4% reduces the communication and storage cost.

References

[1] Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. Applied Sciences, 11(8), 3383.

[2] Blazhevska, K. V. (2022). The Social Security Policy of the Republic of North Macedonia: Reform Process, Opportunities and Perspectives. In Social Security in the Balkans–Volume 2 (pp. 13-33). Brill.

[3] Figueiredo, S. O. D., Sincorá, L. A., Leite, M. C. D. O., & Brandão, M. M. (2021). Determinants of crime control in public security policy management. Revista de Administração Pública, 55, 438-458.

[4] Dong, K., Ali, R. F., Dominic, P. D. D., & Ali, S. E. A. (2021). The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses. Sustainability, 13(5), 2800.

[5] Lingga, P., Kim, J., Bartolome, J. D. I., & Jeong, J. (2021, October). Automatic Data Model Mapper for Security Policy Translation in Interface to Network Security Functions Framework. In 2021 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 882-887). IEEE.

[6] McLeod, A., & Dolezel, D. (2022). Information security policy non-compliance: Can capitulation theory explain user behaviors?. Computers & Security, 112, 102526.

[7] Wong, W. P., Tan, K. H., Chuah, S. H. W., Tseng, M. L., Wong, K. Y., & Ahmad, S. (2020). Information sharing and the bane of information leakage: a multigroup analysis of contract versus noncontract. Journal of Enterprise Information Management, 34(1), 28-53.

[8] Jaeger, L., Eckhardt, A., & Kroenung, J. (2021). The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis. Information & Management, 58(3), 103318.

[9] Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & security, 43, 90-110.

[10] Yazdanmehr, A., Wang, J., & Yang, Z. (2020). Peers matter: The moderating role of social influence on information security policy compliance. Information Systems Journal, 30(5), 791-844.

[11] Muller, S. R., & Lind, M. L. (2020). Factors in information assurance professionals' intentions to adhere to information security policies. International Journal of Systems and Software Security and Protection (IJSSSP), 11(1), 17-32.

[12] Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of information systems, 18(2), 106-125.

[13] Chen, X., Wu, D., Chen, L., & Teng, J. K. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. Information & Management, 55(8), 1049-1060.

[14] Chen, X., Wu, D., Chen, L., & Teng, J. K. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. Information & Management, 55(8), 1049-1060.

[15] Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: a higher education case study. Information & Computer Security.

[16] Brown, D. A. (2017). Examining the Behavioral Intention of Individuals' Compliance with Information Security Policies (Doctoral dissertation, Walden University).