# Model for Cyber Security Information Sharing in Healthcare Sector

1st Jari Hautamäki
*JAMK University of Applied Sciences*
*Institute of Information technology*
Jyväskylä, Finland
jari.hautamaki@jamk.fi

2nd Tero Kokkonen
*JAMK University of Applied Sciences*
*Institute of Information technology*
Jyväskylä, Finland
tero.kokkonen@jamk.fi

***Abstract*— In the modern society almost all services are based on data-networks and networked systems. Especially through the growing digitalization an increasing number of services is connected to data-networks. One example of a highly digitalized domain is the healthcare sector, where a cyber-attack could cause extreme circumstances. Decision making requires knowledge about the current situation. Particularly, in the complex domain of cyber security where the boundaries of physical world do not exist, situational awareness has a determinative role. One source for required cyber security information is obtained by sharing information: different organizations share the information between each other. Typically, Cyber security information has classification levels, which affects challenges for information sharing between different organizations. In this study, the model for information sharing between different organizations with different classification levels is developed and tested in the simulation. Because of its importance, the developed model is tested in the simulation of a healthcare domain; however, it can be utilized in all business sectors. In this paper, not only the developed model with simulation results is presented, but also tested in real life scenarios within an existing project.**

***Keywords—Cyber Security, Situation Awareness, Sharing Situation Awareness, Security Information Sharing***

## I. Introduction

Digitalisation in the healthcare poses great possibilities but there are also new threats. For example, the recently released new version of Finland's Cyber Security Strategy [1] has identified healthcare as a sector the quotidian business of which is out of cyber security; however, healthcare activities are substantially influenced by cyber security, and possible incidents will have devastating impacts. As described in [1], patient information is processed only in electronic format covering all the essential information in the primary healthcare and in the specialized healthcare.

The study [2] classifies healthcare infrastructure as mission critical infrastructure with a great amount of valuable data, hardware and software. Djenna and Saïdouni [3] indicates that within healthcare devices there are significant security issues, and healthcare is a highly targeted sector for cyber-attacks. Study [4] describes generic security cases for information system security in healthcare systems, while Alharam and El-madany [5] describes the security issue with IoT based healthcare systems (complexity of cyber security architecture), while in the study [6] they present the cyber security on healthcare industry. Authors of study [7] present a cyberattack classification with the challenges of cyber security in healthcare sector with the architectural aspects of the secure healthcare network. Safavi et.al [8] reviews the Cyber security trends in healthcare.

In the cyber domain it is extremely important to know the situation of one's valuable assets as the basis of understanding the situation and making decisions based on that understanding. In general, that capability is called Situational Awareness (SA). There are several different definitions for SA [9]. According to the classical Definition of Endsley "Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" [10].

Generally, the number and severity of cyber security attacks is continuously increasing worldwide [11]. The attack methods are constantly evolving, and knowledge of the methods and threats is extremely important to the various players. In such a situation, sharing of information and its secure transmission will play a key role in the fight against cybercrime [12]. One actor's information helps other actors to defend against cyber security attacks efficiently. A key requirement for knowledge sharing is how actors can share information without jeopardizing their own operation. Similarly, the amount of data transmission is quickly growing, and reliability becomes more and more important [13].

With the sharing of information, the information classification should be recognized. There is often a need for organizations to share classified security information, such as security incidents or information about vulnerabilities in their operational systems. Sharing such information always carries a risk. Sharing information requires a confidential relationship between organizations or parties that can be reached in many ways.

The first attempt to address this problem was made by the US Government in 1998 with the publication of a Directive to facilitate the sharing of cyber data [14]. This Directive outlined an operational model for how information sharing in industry can be implemented through Information Sharing and Analysis Centers (ISACs) [15]. Over the past fifteen years, several separate ISAC systems have been created [16].

A problem related to information sharing related is that the information on the intrusion and vulnerabilities cannot generally be used. In the former case, the actor transmitting the information warns other actors when they are compromised. It is often too late to mitigate attacks before serious damage occurs. In the latter case, the vulnerability information is often too general to make prevention activities [17].

Mitre Corporation has released the first versions of following standards for information sharing: Structured Threat Information eXpression (STIXTM) [18] and Trusted Automated eXchange of Indicator Information (TAXIITM) [19]. The later versions of STIX and TAXII have been transitioned to the standard of (OASISTM) Cyber Threat Intelligence (CTI) [20]. Most of these systems focus on sharing information about intrusions and vulnerabilities. In general, such information is sensitive and companies' willingness to share information varies greatly [17].

### A. Motivation and Structure

In our earlier study [21], the first model for sharing information of situational awareness between organisations was introduced. Using the earlier model for creating information sharing topology for STIX and TAXII based infrastructure, it was possible to share classified security related information between multiple organizations with minimal risks. In that earlier model, a non-weighted link scenario with calculation of shortest path by Dijkstra algorithm [22] was used.

There were shortcomings in the first model; hence, it was decided to improve and target it to the healthcare domain. Healthcare domain has its special characteristics with the handled data and regulations with the data, which makes it an extremely interesting and important domain to investigate. In a networked healthcare environment, sharing security information of situational awareness is particularly important. The value of security information increases with use. The value of unused data is reset prematurely. Efficiency in a networked environment means sharing security information and developing an organizational culture.

The paper is organised as follows. In section II, the new improved model is introduced. That new model is tested by using the simulation described in section III. Lastly, in section IV, the study is concluded with found future research topics.

## II. Information Sharing Model

The traditional model of knowledge sharing is based on the so-called Hub and Spoke model. The model faces many challenges, such as legal and constitutional limits, speed of information sharing, trusted relationships and technology [19], [23], [24]. The Hub and Spoke model is illustrated in Fig. 1.

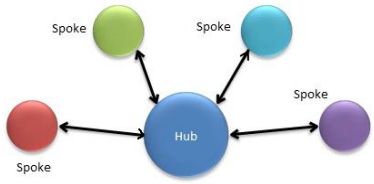


Fig. 1. Hub and spoke model [19]

In the Hub and Spoke model, the Hub has a central role. The Hub receives the information and distributes it to other participants (spokes) in the network. At the same time, it can act as a refiner of knowledge and as a resolver of any questions about knowledge before sharing information. The Hub and Spoke model works well in situations where the network is small and the information sharing is not too time-critical, as the model necessarily delays information passing through the Hub [23].

A more flexible model than the Hub and Spoke is the so called Peer to Peer model, where there is a clear security information distributor. Unlike the Hub and Spoke model, this model does not have any centralized information-sharing organization. The Peer to Peer model is illustrated in Fig. 2.

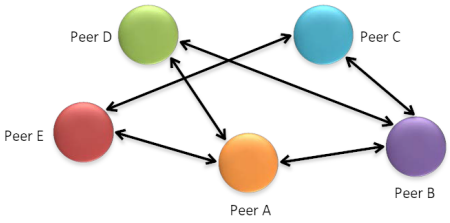


Fig. 2. Peer to Peer model [19]

In this way, information is rapidly transmitted between different actors; also, load balancing and fault tolerance are easier to implement. This model also has its own challenges. In particular, the model highlights the challenge of sharing confidential information and ensuring that information is communicated to all the different parties in the network [25].

This study has addressed the challenges outlined above by developing a new model in which knowledge is shared through a combination of the Hub and Spoke and Peer to Peer models. The model is an improved version of a previously published model in which the data sharing path was determined by the Dijkstra algorithm without taking a position on how the weight of links between different actors, i.e. the risk level of data transmission, is determined [21].

This research model is based on determining the importance of links between organisations to share information through the following equation:

$$W_l = ( L_s + L_d ) \times ( | S_s - S_d | + 1 ) \quad (1)$$

Weight $W_l$ represents the risk value for transmitting information. $L_s$ and $L_d$ in the information sharing network describes the activity level of the sender and destination of the information in the network. In the model, the activity levels are divided into three categories: Enterprise, Operator and National Operator Level (CERT). Each level has its own value. The enterprise-level value is one, the operator- level value is two, and the CERT-level value is three. The most effective information sharing takes place between lowest level organizations like enterprises and second level organizations like ISPs. These levels originate from the principle of the Hub and Spoke model, where the Hub act as the centralized information distributor. Ss and Sd are the sender and receiver definitions for the data protection classification level at each actor level. The lower security classification level specifies, that an actor has more critical information in their organization. In this equation, 1 has been added to avoid a situation where the same classification level of organizations gets the weight number zero to the link between them. Different methods, such as the ISO27005:2018 standard set or the national audit criteria, can be used to determine the level of protection [26]. For example, in Finland, there is an information security audit tool for authorities called KATAKRI [27], which can be used to assess the ability of an organization to protect classified information [28].

When implemented in this way, organizations obtain their own weight for each link between them, which can be used to determine a shortest path for data transmissions. The weight is the same in both directions. Fig. 3. illustrates an example how the weight of the link is calculated.

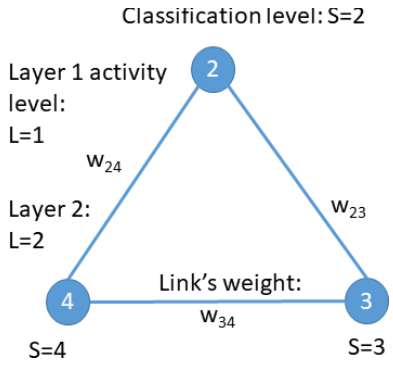


Fig. 3. Links weight example

Weights of the links in Fig. 3. are calculated as follows:

$$W_{24} = ( 1 + 2 ) \times ( | 2 - 4 | + 1 ) = 9$$

$$W_{23} = ( 1 + 2 ) \times ( | 2 - 3 | + 1 ) = 6$$

$$W_{34} = ( 2 + 2 ) \times ( | 4 - 3 | + 1 ) = 8$$

Using this model direct higher-risk connections can be avoided and a safer information sharing network created. This study assumes that all organizations are responsible for defining their own classification level of security for their own information to be shared and thereby determining the level of risk based on the information shared and the associated organization. Organization's which have the same or nearest classification level can trust better to each other. An organization does not need to share information with all other organizations; only to trusted individuals whose risk level has been assessed. The risk level of links describes the network for which the shortest path between organizations can be calculated. The Dijkstra algorithm [22] is used to determine the shortest path in the model.

## III. Simulation of the Model

Let's assume, that a real-life scenario of security information sharing community in healthcare domain has illustrated in Fig. 4. The scenario has been randomly selected to illustrate as wide as possible the different possibilities for building a information sharing network.

For achieving the comparability with earlier simple model, similar simulation scenario is used. In this study the scenario is tailored for healthcare domain. In the scenario there are three different countries with the national CERT. The national CERT acts as the highest authority in the information sharing. The next level is formed by Internet Service Providers (ISP) and the lowest level are local and national healthcare enterprises operating in current country, for example hospitals. The scenario has three ISPs, the first operates only in the country 2 and the second only in the country 3, while the third operates in both of those countries. Every node represents an organisation with individual information sharing service. Value of every link is based on the classification level and risk estimation of shared sensitive information and attached organisation. Risk level has been calculated by the equation 1. If the information sharing is unacceptable, there will be no link between nodes. If accepted, there can be a special situation where the shared information shall flow through ISP or CERT level to enterprises in another country even if enterprises do not share information between countries.

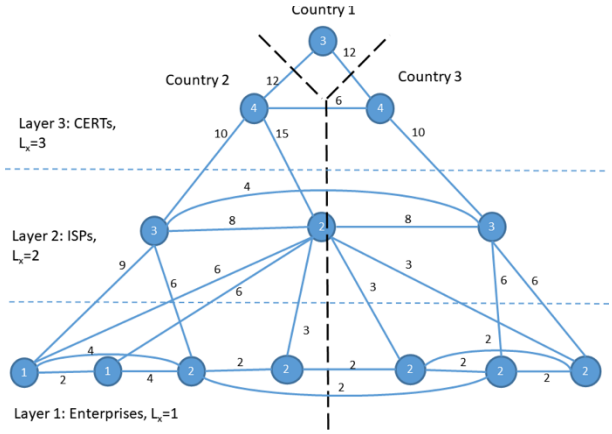


Fig. 4. Real life scenario of security information sharing network

Pseudo code of Dijkstra's algorithm can be presented as follows [29]: Let's assume network $G = (N, E)$ with $N$ nodes and positive distances $D_{ij}$ (risk values in this model) for all edges (i, j ∈ N). The shortest path from $S$ to node $j$ (where start node is $S$ and labelled set of nodes is $P$):

1) *$P = \{S\}$, $D_S = 0$ and $D_j = d_{sj}$ for $j \notin N$ ($j \neq S$)*
2) *find the closest node $i \notin P$ where $D_i = min[D_j]$ and $j \notin P$. Set $P = P \cup \{i\}$, if $P$ contains all nodes stop, else go to 3*
3) *update labels for $j \notin P$, set $D_j = min[D_j, D_i + d_{ij}]$, go to 2*

Now the information sharing topology for the scenario in the healthcare domain can be implemented as in Fig. 5.

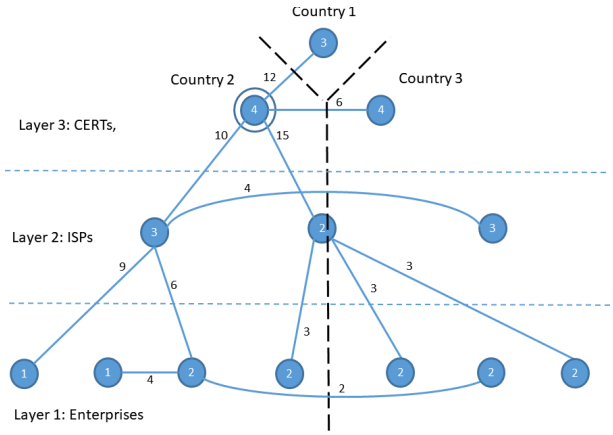


Fig. 5. The Shortest path information sharing network

The model is suitable for use inside one country and with different hierarchical organizations. This example scenario uses different countries with CERT, ISPs and healthcare organisations, because those combine a relevant structure for real life state-of-the-art operations. The scenario proves that our model works as it should and it can be used as a basis for the state-of-the-art cyber security information sharing topology.

With this model, each actor in the data sharing network receives timely information on possible security incidents. At

the same time, the accuracy of the information can be better ensured. The advantage of this combination model is the faster sharing of security-related information (Peer to Peer) than it would be possible using the centralized model alone. At the same time solving information refinement, the problems and more targeted situation information sharing can be better ensured by utilizing the resources of the centralized model (Hub and Spoke). This is particularly the case with public organizations such as health care institutions. For hospitals, sharing information on security incidents is not as critical as for private companies; nevertheless, the availability, accuracy and timeliness of information are particularly important.

## IV. Conclusions

This paper introduces the model for sharing cyber security information between organisations in the healthcare sector. The model is also suitable for other sectors; however, the healthcare sector was chosen because of its importance in the cyber domain. The test simulation proves that the model can be used for real-life scenarios with real classified information. With the demonstration it was also proved that the model can be used inside one country or between countries if ”higher authorities” with international interfaces are involved. Information sharing requires the definition of the classification level of shared information.

It must be stated that the model is more theoretical and requires testing with real data and real systems with carefully defined classification levels for the shared data and involves data-networks and systems because they often restrict the connectivity.

A future work model can be tested in the realistic technical scenario for example by utilising the healthcare cyber range infrastructure. Also, data-analysis and deep learning can be utilised for solving the routing problem of the shared information.

## Acknowledgment

This research is funded by the Regional Council of Central Finland/Council of Tampere Region and European Regional Development Fund as part of the Health Care Cyber Range (HCCR) project of JAMK University of Applied Sciences Institute of Information Technology.

## References

[1] J. Reponen, M. Kangas, P. Hämäläinen, N. Keränen, and J. Haverinen, "Use of information and communication technologies in health care 2017, Situation and direction of development - Tieto- ja viestintäteknologian käyttö terveydenhuollossa vuonna 2017, Tilanne ja kehityksen suunta," http://urn.fi/URN:ISBN:978-952-343-108-9, 2018, accessed: 26 November 2019.

[2] A. Boddy, W. Hurst, M. Mackay, and A. E. Rhalibi, "A study into detecting anomalous behaviours within healthcare infrastructures," in 2016 9th International Conference on Developments in eSystems Engineering (DeSE), Aug 2016, pp. 111-117.

[3] A. Djenna and D. Eddine Saïdouni, "Cyber attacks classification in iot-based-healthcare infrastructure," in 2018 2nd Cyber Security in Networking Conference (CSNet), Oct 2018, pp. 1-4.

[4] Y. He and C. W. Johnson, "Generic security cases for information system security in healthcare systems," in 7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012, Oct 2012, pp. 1-6.

[5] A. K. Alharam and W. El-madany, "Complexity of cyber security architecture for iot healthcare industry: A comparative study," in 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Aug 2017, pp. 246-250.

[6] A. K. Alharam and W. El-Madany, "The effects of cyber-security on healthcare industry," in 2017 9th IEEE-GCC Conference and Exhibition (GCCCE), May 2017, pp. 1-9.

[7] D. I. Dogaru and I. Dumitrache, "Cyber security in healthcare networks," in 2017 E-Health and Bioengineering Conference (EHB), June 2017, pp. 414-417.

[8] S. Safavi, A. M. Meer, E. Keneth Joel Melanie, and Z. Shukur, "Cyber vulnerabilities on smart healthcare, review and solutions," in 2018 Cyber Resilience Conference (CRC), Nov 2018, pp. 1-5.

[9] G. P. Tadda and J. S. Salerno, Overview of Cyber Situation Awareness. Boston, MA: Springer US, 2010, pp. 15-35. https://doi.org/10.1007/978-1-4419-0140-8 2

[10] M. Endsley, "Toward a theory of situation awareness in dynamic systems," Human Factors, vol. 37, no. 1, pp. 32-64, 1995.

[11] L. Hirshfield, P. Bobko, A. J. Barelka, M. R. Costa, G. J. Funke, V. F. Mancuso, V. Finomore, and B. A. Knott, Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications. Hershey, PA: IGI Global, 2019, pp. 1482-1499.

[12] D. Tosh, S. Sengupta, C. A. Kamhoua, and K. A. Kwiat, "Establishing evolutionary game models for cyber security information exchange (cybex)," Journal of Computer and System Sciences, vol. 98, pp. 27 - 52, 2018. http://www.sciencedirect.com/science/article/pii/S002200001630085X

[13] A. Deljoo, T. Engers, R. Koning, L. Gommans, and C. Laat, "Towards trustworthy information sharing by creating cyber security alliances," 08 2018, pp. 1506-1510.

[14] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "The impact of information sharing on cybersecurity underinvestment: A real options perspective," Journal of Accounting and Public Policy, vol. 34, no. 5, pp. 509-519, 2015.

[15] M. He, L. Devine, and J. Zhuang, "Perspectives on cybersecurity infor- mation sharing among multiple stakeholders using a decision-theoretic approach," Risk Analysis, vol. 38, no. 2, pp. 215-225, 2018.

[16] C. Goodwin, J. P. Nicholas, J. Bryant, K. Ciglic, A. Kleiner, C. Kutterer, A. Massagli, A. Mckay, P. Mckitrick, J. Neutze et al., "A framework for cybersecurity information sharing and risk reduction," Microsoft, 2015.

[17] C. Colicchia, A. Creazza, C. Noè, and F. Strozzi, "Information sharing in supply chains: a review of risks and opportunities using the systematic literature network analysis (slna)," Supply Chain Management: An International Journal, vol. 24, no. 1, pp. 5-21, 2019.

[18] S. Barnum, "Structured Threat Information eXpression (STIXTM), white paper, version 1.1, revision 1," http://stixproject.github.io/getting-started/whitepaper/, 2014, accessed: 26 November 2019.

[19] J. Connolly, M. Davidson, and C. Schmid, "The Trusted Automated eXchange of Indicator Information (TAXIITM), white paper," http://taxiiproject.github.io/getting-started/whitepaper/, 2014, accessed: 26 November 2019.

[20] "OASIS STIXTM and TAXIITM documentation," https://oasis-open.github.io/cti-documentation/, accessed: 26 November 2019.

[21] T. Kokkonen, J. Hautamäki, J. Siltanen, and T. Hämäläinen, "Model for sharing the information of cyber security situation awareness between organizations," in 2016 23rd International Conference on Telecommunications (ICT), May 2016, pp. 1-5.

[22] E. W. Dijkstra, "A note on two problems in connexion with graphs," Numerische Mathematik, vol. 1, no. 1, pp. 269-271, Dec 1959. https://doi.org/10.1007/BF01386390

[23] S. N. Khajeddin, A. Madani, H. Gharaee, and F. Abazari, "Towards a functional and trustful web-based information sharing center," in 2019 5th International Conference on Web Research (ICWR), April 2019, pp. 252-257.

[24] F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," Computers & Security, vol. 60, no. C, pp. 154-176, 2016.

[25] M. Parameswaran, A. Susarla, and A. B. Whinston, "P2p networking: an information sharing alternative," Computer, vol. 34, no. 7, pp. 31-38, July 2001.

[26] F. S. A. SFS, Information technology. Security techniques. Information security risk management, ISO SFS-ISO/IEC 27 005:2018, 2018.

[27] Ministry of Defence, Finland, "Katakri, information security audit tool for authorities - katakri, tietoturvallisuuden auditointity√∂kalu viranomaisille," https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf, 2015, accessed: 22 November 2019.

[28] J. Rajamäki, "Challenges to a smooth-running data security audits. case: A finnish national security auditing criteria katakri," in 2014 IEEE Joint Intelligence and Security Informatics Conference, Sep. 2014, pp. 240-243.

[29] X. Li, G. Li, and S. Zhang, "Routing space internet based on dijkstra's algorithm," in 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, vol. 2, April 2010, pp. 118-121.