Human Element Numerous Focused on Data, Threats, Risk, Privacy Management for Smart Cities

Yakubu Ajiji Makeri [1], Albert Meijer [2], Yi Qian [3] Giuseppe T. Cirella [4]
[1]Kampala International University,Kampala,Uganda(yakubu.makeri@kiu.ac.ug)
[2] Utrecht University – School of Governance. The Netherlands. Country (A.J.Meijer@uu.nl)
[3] Department of Electrical and Computer Engineering, University of Nebras-ka-Lincoln (UNL), (yqian@ieee.org)
[4] University of Gdansk, Poland (gt.cirella@ug.edu.pl)

Abstracts
In numerous nations, laws have not stayed aware of the innovation, leaving critical holes .In different nations, law implementation and insight offices have been given critical exceptions. At last, without sufficient oversight and implementation, the simple presence of a law may not give satisfactory protection. The expanding complexity of data innovation with its ability to gather, dissect, and spread data on people who have acquainted a desire to move quickly with the interest for enactment. Moreover, new improvements in clinical exploration and care, broadcast communications, progressed transportation frameworks, and monetary exchanges have significantly expanded the degree of data produced by every person. PCs connected by rapid organizations with cutting edge preparing frameworks can make extensive dossiers on any individual without the requirement for a solitary focal PC framework. New advancements created by the safeguard business are spreading into law authorization, non-military personnel offices, and private companies. Government and resident the same may profit by its plenty of plots being executed by the private and public areas.

Keywords
Security, Data, government. Urban governance

1. Introduction

Innovation has become a significant device for some non-administrative associations (NGOs) and gatherings gathering information in the creating scene. For instance, innovation can furnish individuals in far-off districts with admittance to monetary administrations and permit associations to gather crucial data inside the networks they serve. Data and Communication Technology for Development (ICTD) is the investigation of what innovation can achieve and how innovation is utilized in such low-asset settings around the globe. ICTD takes a wide meaning of "low-asset". Regions influenced by destitution are often the focal point of ICTD, yet any setting where things like restricted network, problematic force, or daintily gifted staff scheme to make a novel mechanical scene may be pertinent to ICTD. Even though there have been a few endeavors to study and address PC security and protection chances with advances in an ICTD climate, both dependent upon the situation for explicit innovations and from a scholastic viewpoint, e.g., (Ben-David et al., 2011, Corrigan-Gibbs and Chen, 2014, Reaves et al., 2015), the space of "PC security meets ICTD" is as yet in its outset. We add to this space through bits of knowledge into how to assess and address PC security chances in ICTD conditions. To give an establishment to our bits of knowledge, we decide to zero in on a specific class of advancements—information assortment toolbox—and, specifically, a particular, generally utilized occasion of such an innovation: Open Data Kit (ODK). Information is critical for some NGOs and analysts to screen and assess arrangements or mediations and report to givers on exercises. For instance, associations may gather persistent data during center visits, evaluate the commonness of irritations in-country farmland, or report a foundation needing a fix. ODK permits computerized structures to be made without profoundly specialized aptitude, and has been utilized as a stage by various associations. By considering PC security chances with ODK, we can extricate exercises for both ODK and other information assortment arrangements, just as construe exercises for other new ICTD advances.

Manuscript received January 5, 2026
Manuscript revised January 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.1.4

1.1 Build up data sharing objectives and targets that help business cycles and security approaches.

An association's data sharing objectives and goals should propel its general network safety methodology and help an association with all the more successfully oversee digital-related danger. An association should utilize the consolidated information and experience of its faculty and others, for example, individuals from digital danger data sharing associations, to share danger data while working per its security, protection, administrative, and lawful consistence prerequisites.

1.2 Distinguish existing interior wellsprings of digital danger data.

Associations ought to distinguish instruments, sensors, and vaults that gather, produce, or store digital danger data, danger investigation stages, and conveyance instruments that help the trading of digital danger data. As inside digital danger data sources and abilities are distinguished, associations ought to decide how data from these sources at present help online protection and hazard the board exercises. Associations ought to likewise archive noticed information holes and consider procuring extra danger data from other (conceivably outer) sources or through the arrangement of different instruments or sensors. At last, associations ought to distinguish dangerous data that is accessible and reasonable for imparting to outside gatherings.

1.3 Determine the extent of data sharing exercises.

The expansiveness of an association's data sharing exercises should be steady with its assets, capacities, and destinations. Data sharing endeavors should zero in on exercises that give the best incentive to an association and its sharing accomplices. The perusing action ought to distinguish kinds of data that an association's key partners approve for sharing, the conditions under which sharing of this data is allowed, and those with whom the data can and should be shared.

1.4 Set up data sharing guidelines.

Sharing guidelines are expected to control the distribution and conveyance of dangerous data, and thusly help to forestall the dispersal of data that, if inappropriately revealed, may have unfavorable ramifications for an association, its clients, or its colleagues. Data sharing rules should mull over the dependability of the beneficiary, the affectability of the mutual data, and the possible effect of sharing (or not sharing) explicit sorts of data.

1.5 Join and take an interest in data sharing endeavors.

An association ought to recognize and take an interest in sharing exercises that supplement its current danger data abilities. An association may have to partake in different data-sharing gatherings to meet its operational requirements. Associations ought to think about open and private sharing networks, government archives, business digital danger data feeds, and open sources, for example, public sites, web journals, and information take care of.

2. Effectively try to enhance pointers by giving extra settings, rectifications, or recommended upgrades.

Whenever the situation allows, associations should build the helpfulness and adequacy of danger data by creating metadata for every pointer that is produced. Such metadata can give a setting concerning the marker by depicting the planned utilization of the pointer, how it is to be deciphered, and how it identifies with different markers. Moreover, sharing cycles ought to incorporate components for distributing pointers, refreshing pointers, and related metadata, and withdrawing entries that are off base or maybe unintentionally shared. Such criticism assumes a significant function in the improvement, development, and nature of the markers shared inside a network.

1.2 Utilize secure, mechanized work processes to distribute, burn-through, investigate, and follow up on digital danger data.

The utilization of normalized information configurations and transport conventions to share digital danger data makes it simpler to computerize danger data preparation. The utilization of mechanization empowers digital danger data.

3. Threat Information Types

A digital danger is "any condition or occasion with the possibility to antagonistically affect hierarchical tasks (counting mission, capacities, picture, or notoriety), authoritative resources, people, other associations, or the Nation through a data framework utilizing unapproved access, demolition, divulgence, or alteration of data, or potentially forswearing of administration." For curtness, this distribution employments the term danger rather than "digital danger". The people and gatherings acting dangers are known like "danger entertainers" or just entertainers. Danger data is any data identified with a danger that may enable an association to ensure itself against a danger or recognize the exercises of an entertainer. Significant kinds of danger data incorporate the following:

3.1 Indicators are specialized antiquities or observables1 that recommend an assault is impending or is presently in progress or that a trade-off may have just happened. Pointers can be utilized to distinguish and shield against possible dangers. Instances of markers incorporate the Internet Protocol (IP) address of a suspected order and control worker, a dubious Domain Name System (DNS) area name, a Uniform Resource Locator (URL) that references malignant substance, a document hash for a malevolent executable, or the headline text of a vindictive email message.

3.2. **Tactics**, methods, and methodology (TTPs) depict the conduct of an entertainer. Strategies are elevated level depictions of conduct, strategies are point by point portrayals of conduct with regards to a strategy, what's more, strategies are even lower-level, exceptionally definite depictions with regards to a strategy. HTTP could depict an entertainer's propensity to utilize a particular malware variation, request of activities, assault instrument, conveyance system (e.g., phishing or watering opening assault), or adventure.

3.3. **Security alarms**, otherwise called warnings, releases, and weakness notes, are brief, typically human-readable, specialized notices concerning current weaknesses, misuses, and other security issues. Security alarms begin from sources, for example, the United States Computer Emergency Readiness Group (US-CERT), Information Sharing and Analysis Centers (ISACs), the National Vulnerability Information base (NVD), Product Security Incident Response Teams (PSIRTs), business security administration suppliers, and security analysts.

3.4. Threat insight reports are by and large writing records that depict TTPs, entertainers, sorts of frameworks and data being focused on, and other danger related data that gives more noteworthy situational attention to an association. Danger insight is danger data that has been totaled, changed, dissected, deciphered, or enhanced to give the fundamental setting to dynamic cycles.

3.5. Tool designs are suggestions for setting up and utilizing apparatuses (systems) that help the mechanized assortment, trade, handling, examination, and utilization of danger data. For instance, apparatus arrangement data could comprise of guidelines on the best way to introduce and utilize a rootkit identification and evacuation utility, or how to make and alter interruption recognition marks, switch access control records (ACLs), firewall rules, or web channel arrangement documents. Numerous associations as of now produce and offer danger data inside. For instance, an association's security group may distinguish malignant documents on an undermined framework when reacting to an occurrence and produce a related arrangement of pointers (e.g., record names, sizes, hash esteems). These pointers may then be imparted to framework overseers who design security instruments, for example, host-based interruption discovery frameworks, to distinguish the presence of these markers on different frameworks. Similarly, the security group may dispatch an email security mindfulness activity in light of a noticed ascent in phishing assaults inside the association. These practices exhibit data sharing inside an association. The essential objective of this distribution is to cultivate comparative danger data sharing practices over hierarchical limits – both securing danger data from different associations, and giving inside produced danger data to different associations.

4. Benefits of Information Sharing

Danger data sharing gives admittance to dangerous data that may somehow or another be inaccessible to an association. Utilizing shared assets, associations can upgrade their security pose by utilizing the information, experience, and abilities of their accomplices proactively. Permitting "one association's discovery to turn into another's prevention"2 is a ground-breaking worldview that can propel the general security of associations that effectively share danger data. An association can utilize shared danger data from numerous points of view. A few uses are operationally arranged, for example, refreshing undertaking security controls for nonstop checking with new markers and arrangements to recognize the most recent assaults and settles. Danger data may likewise be utilized deliberately, for example, utilizing shared danger data as sources of info when arranging significant changes to an association's security design. Danger data traded inside networks coordinated around explicit ventures or areas (or some other shared trademark) can be especially useful because the part associations frequently face entertainers that utilization normal TTPs that focus on similar sorts of frameworks and data. Digital guard is best when associations cooperate to hinder and safeguard against efficient, able entertainers. Such a joint effort assists with lessening hazard and improve the association's security pose. Advantages of data sharing include:

4.1. **Shared Situational Awareness**. Data sharing empowers associations to use the system information, experience, and insightful capacities of their sharing accomplices inside a network of interest, in this way upgrading the guarded capacities of numerous associations. Indeed, even a solitary commitment—another marker or perception about an entertainer—can expand the mindfulness and security of a whole network.

4.2. **Improved Security Posture**. By creating and sharing danger data, associations increase a better comprehension of the danger climate and can utilize danger data to advise their online protection and danger the board rehearses. Utilizing shared data, associations can distinguish influenced stages or frameworks, execute defensive measures, improve discovery capacities, and all the more viably react and recuperate from occurrences dependent on noticed changes in the dangerous climate. As associations share data and thusly moderate dangers, those associations can improve their general network safety pose, in any event, giving a level of assurance to different associations, including the individuals who might not have reacted to the danger data, by diminishing the number of feasible assault vectors for entertainers.

4.3. **Knowledge Maturation**. At the point when inconsequential perceptions are shared and examined by associations, those perceptions can be connected with information gathered by others. This advancement measure expands the estimation of data by upgrading existing pointers and by creating information on entertainer TTPs that are related to a particular occurrence, danger, or danger crusade. Connection can likewise bestow significant bits of knowledge into the connections that exist between pointers.

4.4. **Greater Defensive Agility.** Entertainers ceaselessly adjust their TTPs to attempt to sidestep location, bypass security controls, and adventure new weaknesses. Associations that share data are frequently better educated about changing TTPs and the need to quickly recognize and react to dangers. This mindfulness helps increment their operational rhythm and decreases the likelihood of fruitful assault. Such readiness additionally makes economies of scale for network protectors while expanding entertainers' expenses by compelling them to grow new TTPs.

5. Challenges to Information Sharing

While sharing dangerous data unmistakably has benefits, certain difficulties actually remain. A few difficulties that apply both to burning-through and to delivering danger data are:

5.1. **Establishing Trust.** Trust connections structure the reason for data sharing, however, expect exertion to set up and keep up. Progressing correspondence through ordinary in-person gatherings, calls, or online media can help quicken the way toward building trust.

5.2. **Achieving Interoperability and Automation.** Normalized information organizations and transport conventions are significant structure blocks for interoperability. The utilization of normal configurations and conventions empowers computerization and permits associations, vaults, and apparatuses to trade dangerous data at machine speed. Embracing explicit arrangements and conventions, notwithstanding, can require huge time and assets, and the estimation of these ventures can be significantly diminished if sharing accomplices require various arrangements or conventions. During the guidelines improvement measure, early adopters need to acknowledge the danger that it could be important to buy new apparatuses if huge changes to designs and conventions occur.

5.3. **Safeguarding Sensitive Information**. Exposure of delicate data, for example, controlled unclassified data (CUI) and by and by recognizable data (PII) can bring about monetary misfortune, infringement of sharing arrangements, legitimate activity, and loss of notoriety. Sharing security and occasion data, for example, security logs or output results, could uncover the defensive or criminologist capacities of the association and result in danger moving by the entertainer.

The unapproved exposure of data may obstruct or disturb a progressing examination, imperil data required for future legitimate procedures, or disturb reaction activities, for example, botnet takedown tasks. Associations ought to apply dealing with assignments to shared data and actualize strategies, techniques, and specialized controls to effectively deal with the dangers of exposure of delicate data. Setting up Sharing Relationships When dispatching a dangerous data sharing capacity, the accompanying arranging and readiness exercises are recommended:

- Define the objectives and destinations of data sharing
- Identify inside wellsprings of dangerous data
- Define the extent of data sharing exercises
- Establish data sharing guidelines

• Join a sharing network

• Plan to offer progressing help for data sharing exercises

All through this cycle, associations are urged to talk with topic specialists both inside furthermore, outside their association. Such sources include:

• Experienced network protection staff,

• Members and administrators of setting up dangerous data sharing associations,

• Trusted business partners, gracefully chain accomplices, and industry peers, and

• Personnel is proficient about legitimate issues, inside business cycles, techniques, and frameworks. An association should utilize the information and experience from these specialists to help shape a dangerous data sharing capacity that bolsters its main goal and works under its security, protection, administrative, and legitimate consistency prerequisites. Because of continually evolving chances, necessities, needs, innovation, as well as guidelines, this cycle will frequently be iterative. Associations ought to reevaluate and change their data-sharing abilities varying dependent on evolving conditions. Such a change may include rehashing a few or the entirety of the arranging and readiness exercises recorded previously.

Define Information Sharing Goals and Objectives At the beginning, an association ought to set up objectives and goals that depict the ideal results of danger data partaking regarding the association's business cycles and security arrangements. These objectives and targets will help control the association through the cycle of perusing its data-sharing endeavors, choosing and joining sharing networks, and offering to progress help for data sharing exercises. Because of innovative and additionally asset limitations, it very well might be important to organize objectives, what's more, destinations to guarantee that the main data sharing exercises are performed.

Identify Internal Sources of Cyber Threat Information vital advance in any data sharing exertion is to distinguish possible wellsprings of dangerous data inside an association. By directing a stock of inner danger data sources, an association is better ready to recognize information holes. These holes can be tended to by sending extra apparatuses and sensors or then again by securing danger data from outside danger data feeds or vaults. In huge associations, this stock cycle is likewise a method for finding data that is being gathered furthermore, examined in specialty units over the association that may not be at present mutual inside the association.

6. The way toward recognizing dangerous data sources incorporates the accompanying advances:

• Identify sensors, apparatuses, information feeds, and storehouses that produce dangerous data, and affirm that the data is created at a recurrence, exactness, and precision to help online protection decision making.

• Identify danger data that is gathered and broke down as a feature of an association's constant checking technique.

• Locate danger data that is gathered and put away, yet not broke down or audited on a continuous premise. If an association finds valuable danger data that is being underutilized, strategies of incorporating this data into its online protection and danger the board practices should be investigated.

• Identify danger data that is appropriate for offering to outside gatherings and that could support them all the more successfully react to dangers. The proprietors and administrators of dangerous data sources assume a significant function in the stock cycle, what's more, should be counseled. These workforces comprehend what data is accessible and how it is locally put away; the information trade designs that are upheld; and the question dialects, conventions, and administrations accessible for information recovery. A few sources may store and distribute organized, machine-comprehensible information, while others may give unstructured information with no fixed organization (e.g., free content or pictures). Organized information that is communicated utilizing open, machine-meaningful, standard organizations can commonly be all the more promptly got to, looked at, and dissected by a more extensive scope of apparatuses. Subsequently, the arrangement of the data plays a critical function in deciding the straightforwardness and effectiveness of data use, examination, and trade.

7. Define the Scope of Information Sharing Activities

Associations ought to determine the extent of their data sharing exercises by recognizing the kinds of data accessible to share, the conditions under which sharing this data is allowed, and those with whom the data can and should be shared. Associations should survey their data sharing objectives and targets while checking data sharing exercises to guarantee that needs are tended to. When characterizing these exercises, associations ought to guarantee that the data sources and abilities expected to help every action are accessible. Associations ought to likewise consider seeking after sharing exercises that will address realized data holes. For instance, an association may not have an interior malware examination capacity, yet it might access malware markers by taking an interest in a sharing network. The broadness of data sharing exercises will differ dependent on an association's assets and capacities. By picking a generally restricted extension, an association with restricted assets can zero in on a more modest set of exercises that offers the best benefit to the association and its sharing accomplices. An association might have the option to grow the extension as extra abilities and assets become accessible. Such a steady methodology may assist with guaranteeing that data sharing exercises uphold an association's data sharing objectives and goals, while simultaneously fit inside accessible assets.

Associations with more prominent assets and progressed capacities may pick a bigger introductory extension that considers a more extensive arrangement of exercises on the side of their objectives and targets. The level of robotization accessible to help the sharing and receipt of dangerous data is a factor to consider while building up the extent of sharing exercises. Less computerized approaches or manual approaches, which require direct human mediation, may expand human asset expenses and breaking point the broadness and volume of data that can be prepared. The utilization of robotized trade instruments can help diminish human asset costs, and permit an association to trade danger data on a bigger scope. Mechanized danger data sharing ideas are additionally talked about in segment 4.

7.1. Establish Information Sharing Rules

Before sharing danger data, associations should:

• List the sorts of dangerous data that might be shared.

Taking an interest in Sharing Relationships An association's cooperation in a data-sharing network will ordinarily incorporate a few or all of the accompanying exercises:

• Engage in continuous correspondence

• Consume and react to security alarms

• Consume and use markers

• Organize and store pointers

• Produce and distribute pointers

The accompanying segments portray these exercises in more noteworthy detail. Associations simply beginning their dangerous data sharing endeavors ought to at first pick a couple of exercises to zero in on and ought to consider adding exercises as their data sharing ability develops. Associations ought to get that danger data sharing increases—not replaces—an association's basic online protection abilities, paying little mind to the development of their data-sharing practices.

7.2. Engage in Ongoing Communication

Data sharing networks utilize an assortment of specialized strategies to share dangerous data with their individuals. Most associations can get dangerous data through email records, text-based notifications, and web entrances without framework speculations explicit to data sharing, although the substance got through these conveyance channels may should be physically handled (e.g., "reorder" into apparatuses). Associations with security apparatuses that help standard information configurations can utilize norms based information takes care of that empower semi-robotized ingest, handling, and utilization of danger data. Other data sharing techniques, for example, meetings and workshops, require committed staff and travel. Associations that effectively produce and offer dangerous data are probably going to bring about higher correspondence costs. Interchanges might be occasion driven (i.e., in light of the activities or conduct of an entertainer) or intermittent, for example, fortnightly surveys, video chats, and yearly gatherings. The degree of detail, volume, and recurrence of messages conveyed in comprehensible arrangements differ broadly across data sharing networks. A few networks try to convey the most current danger data with insignificant idleness. Conversely, a few beneficiaries utilizing danger data for moving also, the investigation may lean toward outline information and may have no requirement for close to the constant conveyance of itemized data. To diminish the number of messages created, sharing networks now and then give the alternative of buying into digests (i.e., aggregations of messages after some time stretches) instead of accepting singular messages. An association that has as of late joined a data-sharing network may expect time to incorporate new danger data sources into its current online protection rehearses, arrange security apparatuses, and train chiefs on the best way to decipher and follow up on the danger data. During this increased period, an association ought to counsel any accepted procedures direction offered by a network, notice and gain from the communications of more experienced individuals, and inquiry network upholds assets (e.g., network knowledgebase, FAQs, websites). Network supported preparing occasions additionally give occasions to less develop associations and unpracticed workers to increase down to earth bits of knowledge from talented specialists.

Associations ought to likewise set up enrollment and maintenance measures that diminish staff turnover, what's more, encourage the arrangement of confided in expert connections between sharing networks and associations. Maintenance of gifted staff mitigates the deficiency of institutional information, and jelly interests in training. Ongoing cooperation in a sharing network is fundamental for encouraging trust, building up more grounded connections to different individuals, and consistently improving practices. Associations that effectively take an interest in network supported phone calls and up close and personal gatherings are better ready to build up trust with different individuals and thusly to adequately work together after some time.

8. Consume and Respond to Security Alerts

A data-sharing network may distribute security cautions informing network individuals from arising weaknesses, abuses, and other security issues. Fields that ordinarily show up in security cautions, for example, US-CERT alarms, NVD weakness warnings, and seller security notice include10:

- Brief review/leader synopsis and nitty-gritty portrayal, which would incorporate markers;
- Platforms influenced (e.g., working framework, application, equipment
- Estimated sway (e.g., framework crash, information exfiltration, application hijacking
- Severity rating (e.g., Common Vulnerability Scoring System
- Mitigation alternatives, including lasting fixes as well as transitory workarounds
- References for more data; and
- Alert metadata (e.g., ready creation and change dates, affirmations

Endless supply of a security ready, an association ought to decide whether the alarm came from a trusted, solid source. At the point when cautions begin from obscure or untrusted sources, associations may have to apply more noteworthy investigation and additionally look for free affirmation before making a move. If an alarm is considered trustworthy furthermore, it applies to frameworks, applications, or equipment that the association claims or works; the association should decide a reasonable strategy. While deciding a legitimate reaction, an association ought to portray the general effect of an alarm by surveying variables, for example, the seriousness of the caution, the quantity of influenced frameworks inside the association, the impacts an assault may have on the association's crucial capacities, and any operational impacts identified with the sending of relieving security controls. This appraisal ought to educate the prioritization and approach for reaction activities. Reaction activities incorporate exercises, for example, recognizing also, extricating pointers from an alarm, utilizing markers to create and convey recognition marks, making setup changes, applying patches, advising staff of dangers, and executing or improving security controls. Extricating markers is to a great extent a manual cycle today yet there are clear motivations for mechanizing markers taking care of work processes. Manual handling of markers can be time-consuming, repetitive, blunder inclined, and moderate; computerization of the exercises permits investigators to zero in on the translation of data, instead of routine information controls.

9. Conclusion

In numerous nations, the idea has been melded with Data Protection, which deciphers security as far as the executives of individual data. Outside this fairly exacting setting, security assurance is regularly observed as a method of adhering to a meaningful boundary at how far society can interfere into an individual's undertakings. It can be separated into the accompanying features .A huge retailer is dependent upon a digital assault by a criminal association. A great many Mastercard numbers and account data are taken during a break that goes unfamiliar for a little while. The retailer does not offer dangerous data and depends on its security and location abilities. The retailer's interior abilities demonstrate deficient even with an advanced, directed danger that utilizes custom malware. The penetration is found with Visa organizations examining a rash of Mastercard misrepresentation. The credit card organizations confirm that the shared characteristic in the Mastercard misrepresentation was buys produced using this one retailer. The charge card organizations tell both law authorization and the retailer, and an examination is started. The harms are broad. The retailer tells its clients of the robbery of individual data, yet doesn't deliver subtleties of how the assault was completed. Subsequently, a few different retailers are effectively assaulted utilizing similar strategies in the weeks following the underlying break. The monetary misfortunes acknowledged by the retailers, clients, and charge card guarantors and the standing misfortune to the retailers might have been evaded, in any event to some degree, had the retailers occupied with dynamic sharing of danger data with each other. The aggressor is encouraged by the fruitful assault and advantages from the deferred reaction and absence of a coordination. The aggressor benefits monetarily from the fake movement and can utilize these extra assets to extend the degree and advancement of their activities.

References

[1].Y. BenDavid, S. Hasan, J. Pal, M. Vallentin, S. Panjwani, P. Gutheim, J. Chen, E.A. Brewer Computing security in the developing world: a case for multidisciplinary research NSDR 11, ACM, New York, NY, USA (2011), pp. 39-44

[2].A. Gholami, A.-S. Lind, J. Reichel, J.-E. Litton, A. Edlund, and E. Laure, Design and implementation of the advanced cloud privacy threat modeling, International Journal of Network Security & Its Applications, Vol. 8, No. 2, March 2015. Author’s contributions: I am the main author, identified the privacy threats according to the DPD, and developed a proof-of-concept for the Advanced CPTM methodology.

[3] . A. Gholami and E. Laure, Big data security and privacy issues in the cloud,International Journal of Network Security & Its Applications, Vol. 8, No. 1, January 2016. Author’s contributions: I am the main author, identified the related research and state-of-the-art in the area of big data security and privacy.

[4]. A. Gholami and E. Laure,dvanced cloud privacy threat modeling,The Fourth International Conference on Software Engineering and Applications, CCSIT, SIPP, AISC, CMCA, SEAS, CSITEC, DaKM, PDCTA, NetCoM, pp. 229–239, 2016. Author’s contributions: I am the main author, performed the requirements analysis, devised the design, and implemented the methodology.

[5]. A. Gholami and E. Laure, Security and privacy of sensitive data in cloud computing: a survey of recent developments,The Seventh International Conference on Network and Communication Security (NCS), Wireless & Mobile Networks (WiMoNe-2015), pp. 131–150, 2015. Author’s contributions: I am the main author, classified the related research and state-of-the-art according to the cloud provider activities.

[6]. A. Bessani, J. Brandt, M. Bux, V. Cogo, L. Dimitrova, J. Dowling, A. Gholami, K. Hakimzadeh, M. Hummel, M. Ismail, E. Laure, U. Leser, J.-E. Litton, R. Martinez, S. Niazi, J. Reichel, and K. Zimmermann, “Biobankcloud:

[7].Bhattacharya and Thies, 2011 P. Bhattacharya, W. Thies Computer viruses in urban Indian telecenters: characterizing an unsolved problem NSDR ’11, ACM, New York, NY, USA (2011), pp. 45-50

[8].Brunetteal.,2013
W. Brunette, M. Sundt, N. Dell, R. Chaudhri, N. Breit, G. Borriello Open data Kit 2.0: expanding and refining information services for developing regions HotMobile ’13 (2013)

[9].Cobbet al.,2016C. Cobb, S. Sudar, N. Reiter, R. Anderson, F. Roesner, T. Kohno Computer security for data collection technologies proceedings of the Eighth International Conference on Information and Communication Technologies and Development, ICTD ’16, ACM, New York, NY, USA (2016)

[10].A. Schwartz, M. Bhavsar, E. Cutrell, J. Donner, M. Densm ore Balancing burden and benefit: non-prescribed use of employer-issued mobile devices Proceedings of the Sixth International Conference on Information and Communications Technologies and Development: Notes-volume 2, ACM (2013), pp. 140-143

[11] Forbes (2019). These are the smartest cities in the world for 2019. Accessed on 12.1.2019,

[12].Galdon-Clavell, G. (2013). Not so) smart cities?: The drivers, impact and risks of surveillance enabled smart environments. *Science and Public Policy, 40*(6), 717–723.

[13].Gil-Garcia, J. R. (2012). Towards a smart State? Inter-agency collaboration, information integration, and beyond. *Information Polity, 17*(3), 4), 269–280.

[14]. Gupta, P., Chauhan, S., & Jaiswal, M. P. (2019a). Classification of smart city research-a descriptive literature review and future research agenda. *Information Systems Frontiers, 21*(3), 661–685.

[15]. Jameel, T., Ali, R., & Ali, S. (2019). Security in modern smart cities: An information technology perspective. Paper presented at the 2019 2nd International Conference on Communication, Computing and Digital Systems, C-CODE 2019, 293–298.