

Alma Mater Studiorum Università di Bologna
Archivio istituzionale della ricerca

Towards the Creation of Interdisciplinary Consumer-Oriented Security Metrics

This is the final peer-reviewed author's accepted manuscript (postprint) of the following publication:

Published Version:

Gori G., Melis A., Berardi D., Prandini M., Al Sadi A., Callegati F. (2023). Towards the Creation of Interdisciplinary Consumer-Oriented Security Metrics. New York : Institute of Electrical and Electronics Engineers Inc. [10.1109/CCNC51644.2023.10060733].

Availability:

This version is available at: <https://hdl.handle.net/11585/923398> since: 2023-07-04

Published:

DOI: <http://doi.org/10.1109/CCNC51644.2023.10060733>

Terms of use:

Some rights reserved. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

This item was downloaded from IRIS Università di Bologna (<https://cris.unibo.it/>).
When citing, please refer to the published version.

(Article begins on next page)

This is the final peer-reviewed accepted manuscript of:

G. Gori, A. Melis, D. Berardi, M. Prandini, A. A. Sadi and F. Callegati, "Towards the Creation of Interdisciplinary Consumer-Oriented Security Metrics," *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2023, pp. 957-958.

The final published version is available online at:
<https://dx.doi.org/10.1109/CCNC51644.2023.10060733>

Terms of use:

Some rights reserved. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

This item was downloaded from IRIS Università di Bologna (<https://cris.unibo.it/>)

When citing, please refer to the published version.

Towards the Creation of Interdisciplinary Consumer-Oriented Security Metrics

Giacomo Gori, Andrea Melis, Davide Berardi, Marco Prandini, Amir Al Sadi and Franco Callegati

Department of Computer Science and Engineering

Alma Mater Studiorum - Università di Bologna

Bologna, ITALY

Abstract—Information systems are evolving: IoT devices and Cyber-physical systems (CPS) impact on the security of assets and people in the real world. Old cybersecurity approaches, which focused on seeing humans “as a problem”, could be substitute by new paradigms of seeing humans “as a solution”. Therefore, consumers awareness will be one of the building blocks, as well as initiative that aim to create a set of standardized security metrics that can evaluate the security of systems. In order to do that, researchers need to study which are the essential factors that our future metrics should focus on. In this paper we analyzed this problem over CPS while assuming the consumer perspective. We summarize the state of the art in security metrics and advocate the need for a research effort aimed at taking the field to a new level of formal soundness and practical usability by considering interdisciplinary implications on cybersecurity.

Index Terms—Security metrics, Usable Security, Standardization, IoT, CPS

I. INTRODUCTION

IoT devices are spreading around the world and consumer electronics (CE) are more and more popular in the society. With such a fast growth, ransomware and malware attacks are increasing fast [1], so there is a need to understand how security and privacy are affected and which are the risks associated with these devices. Security concerns represent one of the most important barriers to the adoption of large-scale IoT deployments. The consumer electronic community, until now, focused on technological cybersecurity, seeing humans “as a problem”, whereas some studies [2] suggest to follow a more human-centered approach even if difficult to define.

We studied this problem over Cyber-Physical Systems (CPS), that “integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other”, which are the core of current research and innovation activities¹. They are ubiquitous, taking advantage of IoT devices and involve spheres not limited to production activities but also contexts directly affecting human well-being such as transports, environment, and health. Their complexity calls for an increasing adoption of automation, both in terms of intelligent, autonomic operation of single subsystems, and their orchestration at the infrastructural level.

¹https://www.nsf.gov/news/special_reports/cyber-physical/

Algorithms drive the activation and configuration of components, as well as their interconnection and interaction with the physical world. They make decisions taking into account functional requirements, system and network parameters, and measurements from sensors. Security properties are not factored among these features with the same effectiveness, essentially because their evaluation is hardly structured and objectively distilled in quantitative terms.

In this context, consumers can be seen as the division of the company that decides which CPS to adopt: How would a measurable security knowledge about the system influence the choice? To address the current concerns about security, an ambitious initiative introduced in Europe is to reach standardized security metrics, that comes from the analysis of aggregate data overtime. But what properties should they consider? How they address the complexity of the problem?

We claim that to guarantee fundamental rights to safety of individuals and consumers, in a society facing the widespread adoption of CPS, research should achieve a structured, formal modeling of security properties encompassing all of the relevant disciplines. The model should define metrics that must be implemented as a part of the automated operation of CPS, to assess the compliance of security properties with expected requirements, both in real time then as a prediction of the outcome of changes.

To analyze the topic, this paper starts with a short introduction on the effects of having more awareness about cybersecurity for users and consumers. Then, it introduces security metrics, giving a summary of the state of the art in that field applied to CPS, to outline the gaps in current literature. Finally, it talks about characteristic that metrics should have to reach a multi-faceted results, towards the definition of a more complete and applicable view of the subject, analyzing the impact on consumers and different disciplines.

II. AWARENESS AND STATE OF THE ART

A. Consumer Awareness

Cybersecurity awareness depends on various factors, personality included [3], so it can vary a lot among heterogeneous consumers that could often trade security and privacy for convenience. One example of reactions to data breaches overall [4], shows that 51% of their respondents reported they “Changed password or PIN” after receiving the notification, from which 24% “Closed or Switched Account” and 24%

“Became More Diligent”. The 22% “Took no Action”. The study shows that often customers are not aware of the impact of the data breach, maybe due to the economic relevance of the account [5].

Another interesting work is [6], where a survey results in majority of people following bad practises such as personal information on passwords or opening unknown email or links. That lead to almost 80% of them being victim of phishing emails and infected by malware, changing behaviour and showing higher degree of concern only after the incident. On another survey [7], participants indicate theft as the bigger cyberthreats, whereas phishing and cyber stalking rely only in the minority (from 1 to 2%) even if expert suggest that one of the most important security vulnerabilities is phishing. Also, the majority thinks that the steps needed to protect their online security and privacy is too overwhelming to think about, even if 57% of them personally experienced a cyber-attack.

Another interesting survey is the one in [8], that analyzes aspects of consumers experience with home IoT, participants express high concern about weak password and unsecured wifi password, desiring to have feature for more security, like an assistant for authentication.

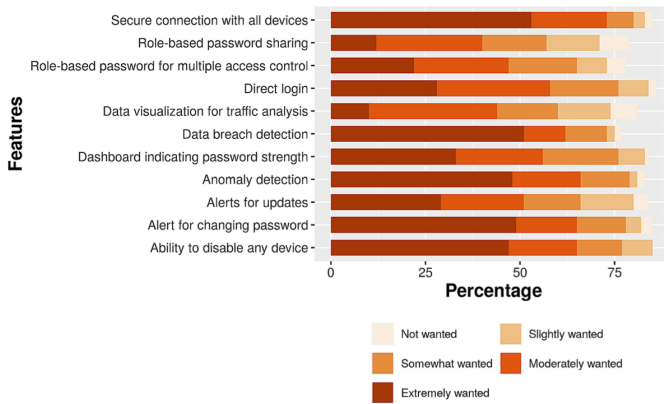


Fig. 1. Likert scale responses for participants' preferences to secure features related to password management for home IoT devices [8]

Then, how would an increased security awareness from consumers affect the adoption of IoT technology? Traditionally it was believed that the more awareness, the less users are prone to the adoption, but work as [9] seems to show a weak, but not negative, impact on the rate of adoption of this technology. Instead, having users not aware of the problematic, with the majority of them not currently concerned and implicitly trust their devices, implies that only manufacturers can address such security issues.

Of course there is no purely technical solution to make systems secure, and for these reasons user behaviour is still a critical attack vector. In [10] is reported that information security is heavily reliant on the behavior of individuals. Awareness is important, that's why we claim the necessity of a security culture in our organizations [11] and society that have to start from early education.

Still, technical mechanisms are essential and consumers prefer to have them to help to deal with their security. Devices that show a clear view of their security level and how to use the features in correct ways could make great improvement to reach this goal. We argue that we need standard metrics that define a common way to evaluate them.

B. State of the Art on security metrics

The reasons for a systematic approach towards security metrics in CPS can be found in recent works such as [12], in which a test is performed to assess how well it can easily meet usable requirements. The results show coverage of almost all desired features, but no metric manages to completely cover all proposed challenges. The most critical gaps regards attack detection and the biggest concerns refer to the fact that the analyzed metrics do not consider dependencies and side effects in System of Systems contexts, mainly focusing on vulnerabilities and attacks.

Papers describing ways of evaluating metrics like [13] mainly deal with system properties, leaving the behaviour of the user mostly uncovered. Surveys were performed, such as [14], which compare many existing proposals regarding system security concluding that significant gaps between the available research results and the desirable metric properties exist. Such properties are sometimes defined with enough clarity for specific sub-fields, as it happens for security metrics for managing industrial automation control systems in the IEC 62443-1-3² standard, which includes what features a good metric should contain.

Some reference texts that define and standardize metrics for measuring security in IT already exists, like ISO 27004³ and NIST 800-55⁴, but they focus on policies and processes, especially made for companies, rather than CPS. We argue that there is a lack of contextualization with currently available metrics.

Initiative like Cybersecurity Act [15] have the goal of establishing a cybersecurity certification framework. However, it has an high degree of heterogeneity of devices to consider, and the context of application may change a lot. For this reason, it can not be considered a fully reliable proposal.

The metrics that we are looking for needs to be

- *Efficient and cost-effective* to make the evaluation rapid, both at design time to avoid delaying of innovations in the market, and at operation time to make the evaluation useful for deployment and reconfiguration purposes.
- Keeping in mind the need of an *agile certification process*, because vulnerabilities can increase over time and the evaluation should be up-to-date during the life-cycle of devices.
- Strike a trade-off between the complexity of the analysis and the need to show an *understandable result* for consumers.

²<https://standards.globalspec.com/std/1671028/dsf-iec-62443-1-3>

³<https://www.iso.org/standard/64120.html>

⁴<https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final>

- Focusing on the evaluation of the *overall systems* and not only single component separately, considering the connections and interaction between them.

Another regard considering the threat environment or not: attackers behaviour could be taken as a training field, getting more precise estimation of security or the amount of damage that a specific attack could produce. For example, if we compare two systems with the same vulnerability that, if exploited, could produce a relatively small damage in the first system but catastrophic in the second, can we say that one is more secure than the other? Should our metrics consider the impact of a possible attack? How to model the environment that metrics will consider?

There is not a simple answer, but we argue that an approach could be to mix environmental depending metrics with the others, developing a model of the environment that considers the involvement of the digital, physical and social worlds.

III. SECURITY FORMALIZATION EFFECTS

Defining a limited, known set of metrics and using it to evaluate systems could lead attackers to have a deeper initial knowledge about systems, gaining hints about which components could be more vulnerable. This suggests a question: is secrecy better or worse than disclosure on security issues? Security should not be dependent on secrecy, also because the disclosure of issues let people and companies take actions to improve defenses. So, in contrast with the intelligence side that is based on secrecy, the cybersecurity world is mainly focused on disclosure (e.g. the MITRE CVE ⁵ classification) and the same principle applies to CPS.

The standardization of security metrics could allow a unified and reproducible view of security in CPS so that the consumer has a clear understanding about the level of security and can compare it with other systems, taking more precise decisions. In addition to bringing more awareness, defining metrics and making an automated assessment of the systems could also allow to understand what are exactly the vulnerabilities that lead to that security score and which countermeasures against attackers are missing.

Threat evaluation and risk analysis are the starting points to build a model linking measurable parameters of the CPS with its features, components, and operational conditions. The attack surface can change over time so that the “security score”, i.e. the output of the analysis, should be up-to-date. Where physical attributes are involved, e.g. printed QR codes that label components for asset management and for initialization of trust relationships, efficient ways should be devised to incorporate security checks on their validity. Freshness of checks must be enforced, as for example PKIs do by placing an expiration date in certificates.

Another implication would be on Cybersecurity Insurance (CI) that is a product, still on the exploring stage, that enable businesses and even consumers to mitigate the risk of cyber

crime activity. Most common automated scans are usually based on already known vulnerabilities. Instead, being able to assess security of devices by standardized security metrics would give useful and precise information to CI traders, with comparable and consistent knowledge on the situation for more precise cost estimation. This could lead to less expensive CI for consumers and less risks for CI traders.

IV. TOWARDS A MULTI-FACETED RESULT

The level of complexity reached by current IT systems makes it necessary to use heterogeneous metrics. The idea of a taxonomy of security metrics that could help bridging different sub-disciplines, is not new [16], yet it has not reached maturity.

Complexity brings also consumption related issues making sustainability and efficiency compelling. Let’s take the example of decision-making algorithms that drive autonomic sub-systems, as well as orchestrators that plan the (re)configuration of infrastructure: they need measurements of specific security properties, continuously available as input. To make this feasible, results should be given in a limited time and with minimum overhead.

Moreover, as we discussed, it’s not just a digital problem. The involvement of not only technical factors, in measuring the security of a system, opens new questions and creates new opportunities and needs for more research, to achieve a multi-faceted result. Especially in CPS that are implicated also in social risks and effect on personal well-being, we claim that it’s important to go beyond the analysis of technical characteristic of systems to consider interdisciplinary aspects.

Discrimination, constraints on freedoms, privacy loss [17] and any other physical or moral harm to people must be considered security properties to be measured.

The goal of this chapter is to give insights and research trends on such topics regarding what we consider the focal driving factors of future security metrics to consider: usability, safety, economics, sustainability and fundamental rights.

A. Usability

Humans interacting with information systems tend to have similar behaviours: things that are easier to do are always preferred. That’s why *usability* measures how easy it is for a consumer to use a product by both considering and the user experience and the security procedures.

Security has a cost and which also influences user experience. For example, security measures like Multi Factor Authentication (MFA) or CAPTCHA can hinder the product usability [18].

Another example relies on the choice of a secure password, which usually conflicts with the usability of a product, but choosing a long and complex password is often a better choice from the security point of view. However, a complex password can be easily forgotten by the consumer and for this reason users frequently choose a simple and easily guessable one [17]

Therefore, more security usually leads on less usability and vice versa: what if it were possible to choose and tune

⁵<https://cve.mitre.org>

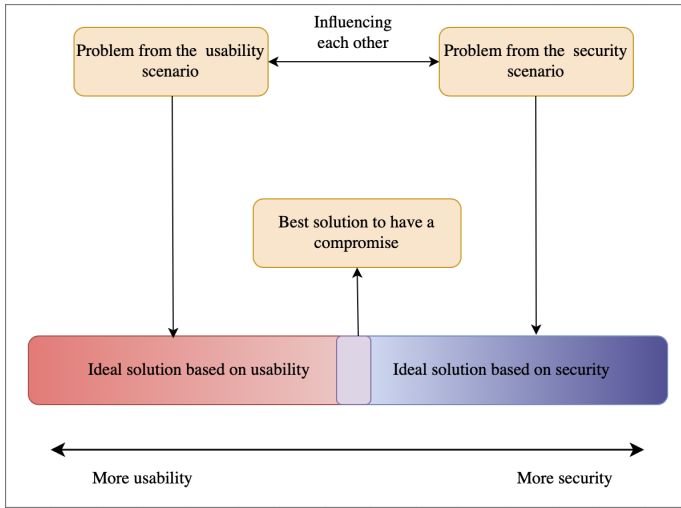


Fig. 2. Usability and Security trade-off: A common solution based on a compromise.

the amount of usability and security to reach an optimal configuration for the consumer?

To achieve that, metrics should consider that high degree of security are not acceptable if they do not ensure a minimum level of usability, that's why there is a need [19] to consider two main aspects of this combined Security and Usability interaction, called "usable security" and "secure usability", to reach an effective security. These metrics should calculate the level of usability, following basic principles [18] such as representing real user behaviours and observing the interactions analyzing the data obtained. Development processes that try to provides both usability and security already exist [20], but we are trying to define a way to measure it, in particular along the development process.

In [21] authors propose a method to combine and summarize usability metrics in a standardized way, obtaining a unique score that still reaches effectiveness and efficiency. This score could drive security metrics on the evaluation of usability.

B. Safety

Safety is not a synonym of Security. While safety aims at protecting life, health and natural environment from any damage that systems may cause, the main goal of security is to protect the confidentiality, integrity and availability of information in the system, threatened by malicious parties [22]. Therefore, secure system do not necessarily need to be safe, and vice versa. For this reason there is a need to measure both aspects. Security and Safety must be considered two side of the same story, especially because they can affect each other. Security algorithms might add crucial delay to the system making it unsafe by slowing the reaction time [23] while some safety procedure could choose to skip some security procedures to grant responsiveness [24].

We argue that there should be a way to estimate the degree of degradation of the safety of a system when security mechanisms are introduced in it. This lead to another constraint

to consider: is safety compromised, and how much, by some security mechanism?

C. The social side

CPS use technologies such as cloud computing or IoT devices that increase the attack surface. However, cybersecurity is not only a digital problem, but it also depends on human interactions which are usually referred to as the "weakest link" [25]. Therefore, we argue that to change radically the way we evaluate the security of systems the real world consumers interactions must be taken into consideration.

Recent cyber-attacks tend to have multi-step approaches where at least one of the phase use social engineering, taking advantage of those "human vulnerabilities" [26]. Metrics that consider only the technical part are not enough [27] since the attackers dynamically adapt the strategy based on the situation. We argue that the economic costs and earnings coupled with the motivations that lead the attacker to pursue a cyberattack are focal properties to take into account to elaborate accurate security analysis.

LeMay et al. [28] propose a state-based model of a system and the adversary representation which considers adversary attack preferences to mimic the strategy and look ahead on the next most promising move for the attacker. The move estimate costs, payoff and probability of detection. In this approach, the model can show the difference in time between attacks made by different types of adversary (APT, nation-state, lone hackers and even employees or administrators).

An example of index that metrics could use is shown in [29], in which risk-analysis and game theory is used to predict if some targets could be really taken into account in attacks.

D. Sustainability

Information systems are central to the operation of most sectors of industrial society [30] and there is an interplay between security decision and energy consumption [31]. The relation between the two requires complex evaluations, e.g.: can a complex defensive strategy, which is apparently resource-costly, be so effective at thwarting attacks as to minimize consumed resources?

Nowadays, sustainability should be a driving force of any decision and many sectors of society will need to rethink their modes of operation, including cybersecurity.

E. Smart cities

CPS are at the center of current research about sustainable IT systems, and a example are Smart Cities: they are based on IoT devices and represents the use of information and communication technology to sense, analyze and integrate the key information of core systems in running cities [32]. They could help in the construction of Smart Transportation systems, Smart Tourism and Smart Urban Management.

In the past 5 years, 2 billion people moved in urban areas and we reached almost the 80% of the world's total energy consumption just with cities themselves [33]. Taking China as an example, the household energy consumption in urban areas

Less developed regions

Africa, Asia (excluding Japan), Latin America and the Caribbean, Melanesia, Micronesia and Polynesia.

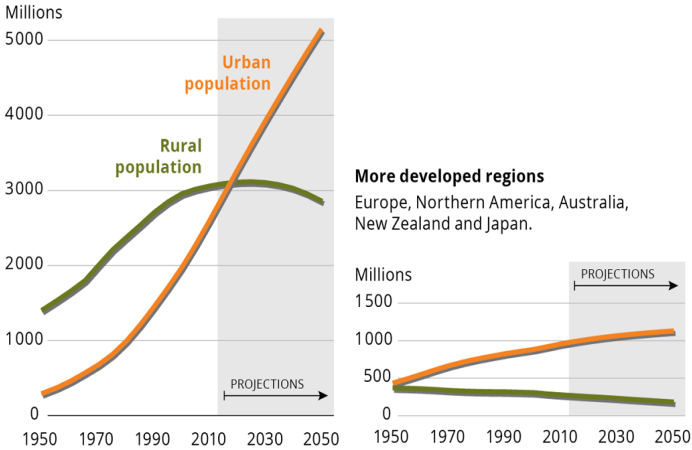


Fig. 3. Changes of urban and rural population shares from 1950 to 2010 and projected until 2050⁷

is always greater than the ones in rural areas, in every region [34].

Smart cities use a management model which mainly focuses on improving urban planning processes to continuously evaluate the resources available. They use data-driven planning in order to provide to their consumers and citizens, an adequate level of quality of life.

This way, smart cities are placed in a strategic position where a lot of energy is used and the "smart component" makes possible to manage resources in efficient way, avoiding wastes, having a central role in the sustainable process.

Smart cities brought big paybacks to users, who are concerned about the privacy of their data. With all of the data that this technology uses, they are also targeted by criminals and prone to be attacked [35], [36], so countermeasures need to be taken.

Cyberattacks on transportation or smart grid systems could stop cities, and even more [37]. This would have a negative impact on sustainability blocking the smart management of resources and services.

As always, deploying security mechanisms comes with a cost: enforcing a countermeasure could be energy-consuming and for this reason the right compromise between consumption and security should be met. Approaches like Network Intrusion Detection Systems (NIDS) could be very energy-demanding in memory and cpu consumption [38]. Some works were designed with the goal of making them more efficient, modeling their resource consumption, changing configuration and testing how the system behaves, especially for mobile systems. [39]. With security metrics that take into account the performance metrics [24], we can modulate the overhead of security depending on the impact on consumption, giving the possibility

to manufacturers and consumers to take more sustainable decisions.

F. A sustainable cybersecurity ecosystem

We argue that cybersecurity is intertwined with sustainability. They influence each other and because of that they should always be considered together every time.

Malicious online activities are constantly increasing and are among the most dangerous [40]. To stop them, a sustainable cybersecurity ecosystem is crucial in terms of saving and securing organizations from being exploited or suffer data breaches, which often afflicts consumers all over the world [41]. To build this ecosystems, the metrics that we are seeking are essential because they can show a well evaluated trade-off between the security level and the resource consumption.

Those metrics could evaluate the use of emerging technologies like IoT and blockchain, that could bring new sustainable cybersecurity approaches needed in this ecosystem. Some examples related to the blockchain technology [42] are:

- *Authenticating critical data* that is stored in a decentralized way.
- *Secure data storage*, by keeping cloud data intact and tamper proof with the use of list of hashes that allows secured and verified data extraction and exchange.
- Use of *absolute records of DNS* via encrypted and secured techniques addressing the concerns that led to the slow adoption of DNSSEC. [blockchain backed DNSSEC]
- *Keyless signature infrastructures*, taking advantage from the timestamp in blockchain, avoid key disclosure, update and revocation.

We have to keep in mind that usually the blockchain introduces intensive computations, especially the ones that reach consensus via the Proof of Work methodology. Different strategies, like Proof of stake and more sustainable alternatives [43] are already being studied to counteract this problem.

V. CONCLUSIONS

In a technology-dependent world, cybersecurity concerns have attracted ever-increasing interest from companies, regulatory bodies, end-users and consumers. The awareness in this field increases every day, especially in respect to the victims of cyber attacks. In fact, Europe is taking the challenging road to establish a cybersecurity certification framework, that will require standardized metrics to evaluate systems. Since cybersecurity is not only a digital problem but involves also the physical and social world, the metrics that will be chosen and created need to meet heterogeneous requirements. CPS mix effects on personal and social risks, involving any kind of life aspects. For this reason usability, safety, social implications and sustainability should be the driving factors to be considered when evaluating the security of systems. A strong analysis of existing solutions and problems should drive deeper researches in this field, opening the door to cross-cutting contributions for cybersecurity.

⁷<https://www.eea.europa.eu/data-and-maps/figures/urban-and-rural-population-in>

REFERENCES

- [1] A. McLean, "IoT malware and ransomware attacks on the incline: Intel security," 2015.
- [2] R. Rohan, S. Funilkul, D. Pal, and H. Thapliyal, "Humans in the loop: Cybersecurity aspects in the consumer iot context," *IEEE Consumer Electronics Magazine*, vol. 11, no. 4, pp. 78–84, 2021.
- [3] A. T. Shappie, C. A. Dawson, and S. M. Debb, "Personality as a predictor of cybersecurity behavior," *Psychology of Popular Media*, vol. 9, no. 4, p. 475, 2020.
- [4] J. Nield, J. Scanlan, and E. Roehrer, "Exploring consumer information-security awareness and preparedness of data-breach events," *Library Trends*, vol. 68, no. 4, pp. 611–635, 2020.
- [5] L. Ablon, P. Heaton, D. C. Lavery, and S. Romanosky, *Consumer attitudes toward data breach notifications and loss of personal information*. Rand Corporation, 2016.
- [6] N. Ahmed, U. Kulsum, I. Bin Azad, A. S. Z. Momtaz, M. E. Haque, and M. S. Rahman, "Cybersecurity awareness survey: An analysis from bangladesh perspective," in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, 2017, pp. 788–791.
- [7] D. Sarathchandra, K. Haltinner, and N. Lichtenberg, "College students' cybersecurity risk perceptions, awareness, and practices," in *2016 Cybersecurity Symposium (CYBERSEC)*, 2016, pp. 68–73.
- [8] A. Alam, H. Molyneaux, and E. Stobert, "Authentication management of home iot devices," in *International Conference on Human-Computer Interaction*. Springer, 2021, pp. 3–21.
- [9] A. A. Harper, "The impact of consumer security awareness on adopting the internet of things: A correlational study," Ph.D. dissertation, Capella University, 2016.
- [10] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237–248, 2014.
- [11] I. Corradini, *Building a cybersecurity culture in organizations*. Springer, 2020, vol. 284.
- [12] A. Aigner and A. Khelil, "A benchmark of security metrics in cyber-physical systems," in *2020 IEEE International Conference on Sensing, Communication and Networking (SECON Workshops)*. IEEE, 2020, pp. 1–6.
- [13] R. K. A. Ahmed, "Security metrics and the risks: an overview," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 41, pp. 106–112, 2016.
- [14] M. Pendleton, R. Garcia-Lebron, J.-H. Cho, and S. Xu, "A survey on systems security metrics," *ACM Computing Surveys (CSUR)*, vol. 49, no. 4, pp. 1–35, 2016.
- [15] J. L. Tran, "Navigating the cybersecurity act of 2015," *Chap. L. Rev.*, vol. 19, p. 483, 2016.
- [16] R. M. Savola, "Towards a taxonomy for information security metrics," in *Proceedings of the 2007 ACM Workshop on Quality of Protection*, ser. QoP '07. New York, NY, USA: Association for Computing Machinery, 2007, p. 28–30. [Online]. Available: <https://doi.org/10.1145/1314257.1314266>
- [17] D. Berardi, F. Callegati, A. Melis, and M. Prandini, "Password similarity using probabilistic data structures," *Journal of Cybersecurity and Privacy*, vol. 1, no. 1, pp. 78–92, 2020.
- [18] M. F. Theofanos and S. L. Pfleeger, "Guest editors' introduction: Shouldn't all security be usable?" *IEEE Security Privacy*, vol. 9, no. 2, pp. 12–17, 2011.
- [19] O. Gordieiev, V. Kharchenko, and K. Leontiev, "Usability, security and safety interaction: profile and metrics based analysis," in *International Conference on Dependability and Complex Systems*. Springer, 2018, pp. 238–247.
- [20] I. Flechais, C. Mascolo, and M. A. Sasse, "Integrating security and usability into the requirements and design process," *International Journal of Electronic Security and Digital Forensics*, vol. 1, no. 1, pp. 12–26, 2007.
- [21] J. Sauro and E. Kindlund, "A method to standardize usability metrics into a single score," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '05. New York, NY, USA: Association for Computing Machinery, 2005, p. 401–409. [Online]. Available: <https://doi.org/10.1145/1054972.1055028>
- [22] M. Bartnes, "Safety vs. security?" 2006.
- [23] M. L. Winterrose, K. M. Carter, N. Wagner, and W. W. Streilein, "Balancing security and performance for agility in dynamic threat environments," in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2016, pp. 607–617.
- [24] R. Fujdiak, P. Mlynek, P. Blazek, M. Barabas, and P. Mrnustik, "Seeking the relation between performance and security in modern systems: Metrics and measures," in *2018 41st International Conference on Telecommunications and Signal Processing (TSP)*, 2018, pp. 1–5.
- [25] B. K. Wiederhold, "The role of psychology in enhancing cybersecurity," pp. 131–132, 2014.
- [26] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social engineering attack strategies and defence approaches," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2016, pp. 145–149.
- [27] D. Gollmann, C. Herley, V. Koenig, W. Pieters, and M. A. Sasse, "Socio-technical security metrics (dagstuhl seminar 14491)," *Dagstuhl reports*, vol. 4, no. 12, p. 28, 2015.
- [28] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke, "Model-based security metrics using adversary view security evaluation (advise)," in *2011 Eighth International Conference on Quantitative Evaluation of SysTems*, 2011, pp. 191–200.
- [29] A. Buldas, P. Laud, J. Priisalu, M. Saarepera, and J. Willemson, "Rational choice of security measures via multi-parameter attack trees," in *Critical Information Infrastructures Security*, J. Lopez, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 235–248.
- [30] B. Penzenstadler, A. Raturi, D. Richardson, and B. Tomlinson, "Safety, security, now sustainability: The nonfunctional requirement for the 21st century," *IEEE Software*, vol. 31, no. 3, pp. 40–47, 2014.
- [31] "From green to sustainability: Information technology and an integrated sustainability framework," *The Journal of Strategic Information Systems*, vol. 20, no. 1, pp. 63–79, 2011, the Greening of IT. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S096386711000035>
- [32] K. Su, J. Li, and H. Fu, "Smart city and the applications," in *2011 International Conference on Electronics, Communications and Control (ICECC)*, 2011, pp. 1028–1031.
- [33] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garcés, "Chapter 12 - cybersecurity, sustainability, and resilience capabilities of a smart city," in *Smart Cities and the un SDGs*, A. Visvizi and R. Pérez del Hoyo, Eds. Elsevier, 2021, pp. 181–193. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B9780323851510000129>
- [34] S. Wang, S. Sun, E. Zhao, and S. Wang, "Urban and rural differences with regional assessment of household energy consumption in china," *Energy*, vol. 232, p. 121091, 2021.
- [35] B. Hamid, N. Jhanjhi, M. Humayun, A. Khan, and A. Alsayat, "Cyber security issues and challenges for smart cities: A survey," in *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, 2019, pp. 1–7.
- [36] A. Melis, M. Prandini, S. Giallorenzo, and F. Callegati, "Insider threats in emerging mobility-as-a-service scenarios," in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.
- [37] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 220–225.
- [38] H. Dreger, A. Feldmann, V. Paxson, and R. Sommer, "Predicting the resource consumption of network intrusion detection systems," in *Recent Advances in Intrusion Detection*, R. Lippmann, E. Kirda, and A. Trachtenberg, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 135–154.
- [39] F. P. Merlo Alessio, Migliardi Mauro, "Measuring and estimating power consumption in android to support energy-based intrusion detection," *Journal of Computer Security*, vol. 23, no. 5, pp. 611–637, 2025.
- [40] F. B. Mariarosaria Taddeo, "We must treat cybersecurity as a public good. here's why," *World Economic Forum*, 2019.
- [41] S. Sadik, M. Ahmed, L. F. Sikos, and A. K. M. N. Islam, "Toward a sustainable cybersecurity ecosystem," *Computers*, vol. 9, no. 3, 2020. [Online]. Available: <https://www.mdpi.com/2073-431X/9/3/74>
- [42] F. Dai, Y. Shi, N. Meng, L. Wei, and Z. Ye, "From bitcoin to cybersecurity: A comparative study of blockchain application and security issues," in *2017 4th International Conference on Systems and Informatics (ICSAI)*, 2017, pp. 975–979.
- [43] A. Li, X. Wei, and Z. He, "Robust proof of stake: A new consensus protocol for sustainable blockchain systems," *Sustainability*, vol. 12, no. 7, p. 2824, 2020.