Human Factor & Artificial Intelligence:

For future software security to be invincible, a confronting comprehensive survey

Bayan O Al-Amri[1], Hatim Alsuwat[2] and Emad Alsuwat[1],
Bayan.o.amri@gmail.com, Hssuwat@uqu.edu.sa, Alsuwat@tu.edu.sa,
[1] Department of Computer Science, College of Computers and Information Technology, Taif University, Saudi Arabia
[2] Department of Computer Science, College of Computer and Information Systems, Umm Al Qura University, Saudi Arabia

Summary
This work aims to focus on the current features and characteristics of Human Element and Artificial intelligence (AI), ask some questions about future information security, and whether we can avoid human errors by improving machine learning and AI or invest in human knowledge more and work them both together in the best way possible? This work represents several related research results on human behavior towards information security, specified with elements and factors like knowledge and attitude, and how much are they invested for ISA (information security awareness), then presenting some of the latest studies on AI and their contributions to further improvements, making the field more securely advanced, we aim to open a new type of thinking in the cybersecurity field and we wish our suggestions of utilizing each point of strengths in both human attributions in software security and the existence of a well-built AI are going to make better future software security.

Key words:
Cybersecurity; ISA; Software Security; Artificial intelligence; Human Factor.

1. Introduction

Over the years there has been a huge contribution and effort to enhance information and software security, varied from error fixings and analyzing previous attacks to prevent potential future ones to evaluating individuals' performances in organizations towards information security and so much more methods with the ultimate goal of strengthening cybersecurity.

With technological development, cybersecurity is also put at the risk and even the new advancements and security strategies of the professionals fail. A Human being is such a wonderful and complex creature, with a mind of unlimited potentials, investing in such a powerful mind has proven not to be wasted in any science, but with all that it will provide, it also may be dangerous to trust sometimes, as we mentioned before, humans are complex, hard to predict in some cases when an individual is under any sort of a circumstance to commit an attack or do harm to an organization either by mistake or on purpose, the cost of that will be huge, as Jouini explained that the costs can variant from tolerant minor damages to a complete information system damages[1], especially if this harm was caused by an internal element that knows the vulnerabilities and keys to breaches to the software security system.

As per some experts, combining the strength of artificial intelligence with cybersecurity, it is possible to defend vulnerable networks and data from attackers. According to the survey conducted by Capgemini research institute, a lot of organizations are turning towards AI-based methods of cybersecurity. This is because of the fact that data security is now more important than ever, however, the non-AI solutions of cybersecurity are proved to fail at some point. The question we are trying to ask is, in the future cyber-security field, can we reduce the chances of such attacks occurring by increasing AI performance? And how much authority privilege are we going to provide the machine with to achieve that? How good and dependable the current individual's security awareness? How smart has machine learning become? This paper addresses some of the results of research relating to such questions about human and machine performances in the cyber-security field.

2. Human Factor in Cybersecurity Field

Since the beginning of technology evolving there were a lot of studies measuring human performance and nature towards software security, one of the latest studies were in 2017 presented by authors in [2], their aim was to inspect the connection between people's Information Security Awareness (ISA) and their variance differences, which to be precise: age, gender, personality, and impulsiveness susceptibility [2].

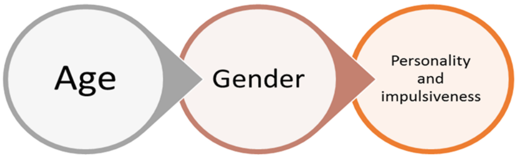

Fig. 1 Human variances connecting to ISA

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.32

Information security awareness (ISA) represents the level of awareness that individuals or systems act upon to protect information security or follow the policies regarding such protection measures against cyber-attacks [2] [3].

Building this level of awareness is measured through testing the tradeoffs of attitude and behavior, and that testing was performed on 505 employees conducted by the Human-Aspects-of-Information-Security-Questionnaire (HAIS-Q) [2], grounded on the triad of KAB (knowledge, attitude, and behavior)

Authors in their research wanted to help to illuminate the differences individuals have in relating to ISA in organizations [2].

It has been reported that in the year 2014/2015, cyber-attacks increased by 38% with cost reaching $2.5 million [2] [4], such huge costs were noticed to have happened mostly due to the malicious acts that came from within the organization in a percentage of 34% of employees' behavior, exceeding the number of external malicious acts [4] [2].

Proving that the current information security measures are not effective enough to enhance the security of the organization [2] [5] [6,7].

This indicates the necessity for focused attention and for a better understanding of human characteristics regarding information security [8].

ISA & KAB Models! Highlights and Results of Questionnaire

Authors [2] built the research based on conjectural and practical influences, the results can help organizations to pinpoint weaknesses and develop practical solutions and procedures to reduce them, plus making advances to enhance training programs for their employees [2].

They mentioned that their work helps theoretically creating a chance to recognize and calculate the variants in employees reacting to ISA but said that there is still a need for further research supporting this particular field of information security [2].

Individuals in an organization's recognition of significant and associations of information security policies, and instructions, are of the focus areas of ISA, along with acting accordingly to what these policies imply [9].

The test studies described individuals that are responding differently to ISA among the test-takers in the next elements:

- Conscientiousness
- Agreeableness
- Impulsiveness susceptibility

While there were no strong and exact specifications about gender and age yet, researchers noted that there is still be a need for more studies regarding these elements reacting in accordance with ISA for more improvements to be applied to training programs [2].

The authors presented the test results highlighted as some main criteria, beginning with Individual characteristics, where it is important to understand the variant characteristics between Individuals, and how they are affecting how they interact psychologically according to ISA [10] [2]. Results were explained through two categories:

1) Gender and Age

A test was presented to observe how gender variance could be part of the elements affecting ISA, high scores were counted on females regarding ISA compared to male test scores [2].

It was also noted that older individuals had higher ISA results, compared to younger employees, a fractional association was performed to examine whether there was the relationship to impulsiveness susceptibility connecting between ISA and age, and indeed there were some variant results suggesting that such a relationship exist [2].

Young employees had lower ISA results, comparing with older individuals, yet this association was properly linear, ISA results amplified with young individuals growing older, said the author that this was stated by Pattinson et al. (2015) [11] [2], when he stated that regarding information security, older individuals are less likely to be risk inclined, Sheng et al[12] stated that phishing emails were more likely to be easily targeting individuals from ages 18 to 35, unlike older users who were less vulnerable to such attacks [12] [2].

Though in relation to gender, the connection between ISA and age persisted substantially even when impulsiveness susceptibility was kept under control, when males had less Information Security Awareness results compared with females, however, this was significantly a slight difference [2].

This slight difference was also noticed in a study showing that males were less likely to be vulnerable to phishing emails unlike females who were slightly more susceptible to such attacks [12] yet there still be a need for more research regarding ISA and gender variances [2].

2) Individual Character and Impulsiveness Susceptibility

Deterioration studies were directed to examine the effect of character, individual variances, and impulsiveness susceptibility on ISA. To start with the character, the results showed that people who are extra careful, sociable, and less likely to fall for impulsiveness, gained more Information security awareness results, therefore, deterioration studies showed that carefulness, affability, and impulsiveness propensity, and mental steadiness were of a notable effect differing on Information Security Awareness.

Cellar et al. (2001), stated that people with good results in carefulness and affability had fewer mistakes in their work.

Authors believe that the studies built upon individuals answering questionnaires by themselves would not be exactly accurate, because of the element of self-preferences, but because the study can be a little affected by that, test-takers were told that their names and their managers' names would be anonymized, and all results will preserve total privacy and identity secrecy [13] [2].

Many kinds of research on this topic weren't as comprehensive in respect to the vastly different aspects in people, people have so many differences based on too many factors, origins backgrounds as an example can be of a big influence on safety issues in systems, and employee's performances[14] [2]Author stated that there are some more aspects that haven't been discussed in the study where those aspects would have an effect on Information Security Awareness, like training programs related to information security [2],

The work primarily concentrated on the BIG FIVE personality aspects, yet there is a need for future works inspecting more about carefulness and affability, authors suggested more studies regarding Information Security Awareness relationship to people's variances in more aspects and approaches that can help reduce the safety concerns that may endanger organizations cybersecurity, Moreover, with all given results of current and previous studies, more researches are needed, authors also stated that in their upcoming research they might discuss in details tow of the main elements of the current study, carefulness, and affability, qualities like "law devoutness", "uniformity" are on the top list of their future examinations. Furthermore, with other personality traits, to support their next study, such as computer knowledge, daily internet access average for every person, such data could be more helpful in understanding more individual differences and their relationships to Information Security Awareness.

Because of the observed relationship that connects the ISA with age variance, more research is required to serve this topic, plus the impulsiveness susceptibility [2]. Noting that some aspects, such as administrative training procedures, were not included in their studies, it is suggestible that these aspects are of a major effect on the security variances of people, [14]

Another study was presented to classify the cybersecurity threats, showed the human element as one of the main threats affecting cybersecurity along with other non-human factors but we are going to address only the human element classification according to what the authors [1] presented:

They essentially classified threat taxonomy based on two categories:

- based on attacks methods
- based on threats bearings

Then they addressed the human element as one of the three elements imposing the information system to threats [1]. Applying proper procedures to avoid attacks are required from supervisors, so they need to inspect for threats that could endanger the organization in terms of information security [1]

Once a weakness point happens to exist in any system, it opens up a chance for a security violation to occur causing unwanted outcomes [15] [16] [1].

McCue in [17] in his study showed that attacks performed on organizations were 70% caused by someone from inside the facility, yet 90% of security measures were fixated on threats that may come from outside of the facility [1].

Alhabeeb [16] when classified security threats in his research, considered three aspects, one is relating to the human factor which is the previous understanding for target systems by adversaries, explaining that in this type of behavior, the adversary collects knowledge about the target system's components and more knowledge about the responsible person and how much knowledge they have about their system, [16] [1], although such sorting may help to understand the threats in a better-classified view it doesn't necessarily be of big help to some establishments with a fast pace of regular nature shifting, adding that many establishments don't succeed preventing breaches that comes from inside the establishment [15] [1].

As a result, human behavior can be sorted into several types of classifications, based on elements such as intensions, and results [1], yet after all these studies we still agree that the human element represents one of the major weaknesses that threaten software security, at least for the time being.

3. Machine learning and Artificial intelligence

Human knowledge has made it possible to make life much easier, faster, more advanced, and practical. Artificial Intelligence (AI) is quite an outstanding example, AI has made a tremendous evolution in the technology field in latest years, the world is evolving in so many ways, medical, educational, economical, entertainment and daily life details, and in military aspects too.

Authors [18] stated after examining research on AI, they measured the huge technology evolution in so many approaches and aspects in deployment time of artificial intelligence and the internet, explaining that it is going to open new opportunities for more advanced prototypes and resources, and ecologies in the industrial field, plus an evolution of artificial intelligence. Adding, that the era of vast advancement of these technologies is reaching a tremendous level, yet they are positively foreseeing that this evolution in artificial intelligence and internet is derived pervasively by many factors they mentioned in their research such as for example "shared services" is going to prove more advancements [18].

This continuous evolution of artificial intelligence and web applications and other advancing technologies are of a big component in this time, an advancement that will play a big role in the renovation of prototypes and resources, and ecologies, serving many aspects such as businesses, health, and security [18]. Current improvements of technological applications globally, the unstoppable use of the web, and many more benefits of advancements, starting to present new paths and application areas in the field, merging elements such as awareness with information into people and renovation physical and cyber environments, all that is producing artificial intelligence to a new stage of innovation, this innovation is upgrading AI into AI 2.0 [19] [18].

In the past decades, AI has evolved into a useful and powerful tool that makes machines act and think like humans. AI is considered the biggest significant shift in technology after mobile and cloud development. It is also estimated that these technologies will take about $1.2 trillion from the competitors that would employ these technologies. With the identification of cat videos to the self-driving cars, several companies are trying to solve and develop the AI strategy. It is said that most of the goals on the basis of which the AI journey initiated are now achieved. This new version of artificial intelligence comprises many developments such as an instinctive insight of information, giving capabilities of concentrated learning, smart internet-derived groups, smart improved tech-derived of human-automated applications (Pan, 2016) [18] [19]

A non-stoppable innovation of intelligent metropolises, smart health systems, smart-transportations, smart robots, smart-entertainments, smart-cars, intelligent-mobile phones, intelligence-based businesses, and many more to mention about how for artificial intelligence application has to offer [18].

Responding to the demands of the current of more applications of artificial intelligence is going to make a huge advancement in the near future, in almost every aspect of daily life, including software and information security.

Understanding AI from Theoretical Perspective

A widely known issue in artificial intelligence regarding the demand of an advanced system to thoroughly clarify choices to individuals and how secure the system is, professionals are required to clarify the reason why it is safe and secure, therefore, the primary objective is to gain people’s confidence [20]. Author [20], in his work, has analyzed the relationship between clarity and confidence in a technological scientific manner, employing results into artificial intelligence and cybersecurity. Argued the significances of investigations in an ethical manner, regarding the incognizant of both approval and disapproval, and the related set accountabilities [20].

How we permit and depend on someone in daily life is usually affected by our confidence of what will they persuade us to believe what they can achieve, like for example, how do we depend on the safety of a product after listening to some assuring facts about it that makes it dependable and trustworthy [21] [20], usually this is the way confidence is attained, the way we introduce the ability to be or not being trustworthy to people or users of some service [20], the main goal is to concentrate on both communications in the cyber field, especially when both clarity and confidence are required in the cyber world a lot [20]. The term 'trust refers to digital trust in the cyber environment, and it gained lots of attention on whether or not is it possible [22] [20].

Author [20], adopted the potential of "e-trust" to be valid deriving from the supposition that confidence originating from the notion that says: “expectations which may lapse into disappointments” [20].

Yet not all rules of daily life about confidence could fit in the cyber-world terms and conditions, the absence of physical existence in the cyber world is one of its conditions that require a different way to clarify facts to users and attain “e-trust” [20]. Regarding artificial intelligence, investigations were executed on smart systems, which are the type of systems that do analyze and propose resolutions about issues that are requiring a real person's knowledge to fix [20]. Issues like health-related choices, economical instructions, manufacture investigations [20], so there will be some exceptions in some points for systems to claim decision support from outside the smart system, as well as comparing the new issues to past ones in aim to resolve them from inside the system [20].

And because this concept has quite a huge attention in the field, a significant number of research were presented to serve more knowledge about it [23] [20].

Remains the issue where it presents a challenge for professionals to obtain people’s trust towards such smart systems and how to show the whole picture of the security operations performed by such smart systems? How secure it can be? Therefore, clarity for people regarding such details to obtain e-trust is subtly anticipated as it’s important to build a strong connection between 'real security and 'supposed security [20].

The difference between clarifications in AI security systems and regular information security systems is that in artificial intelligence they are delivered by AI smart system, while in regular information security system they'll be delivered by engineers [24] [20].

However, the clarification process in both systems is of a big value to make people feel confident about the security in the systems they are dealing with, this requires a deep consideration of the strong relationship between clarification and e-trust [20].

A. Clarifications and e-trust in Artificial Intelligence

In artificial intelligence systems, the major significant objective is validation, presenting details about every act the system performs, the causes behind choices that have been taken, analyses, and suggestions, all must be addressed in details to the user [20]

There is a term that is called a black box, it is used in smart systems and security-superficial systems that is usually pointed out in the cases of unclear clarifications [25] [20], primarily, the idea of a black box Is the uncertainty about enough details-driven into the relationship between clarification and e-trust. Nevertheless, this idea would vary based on the semantics used in the system [20].

Yet in artificial intelligence security systems, this term does not certainly represent an issue, On the assumption that people are trusting the security provided by the system, in this case, not much attention they will pay for such professional details or clarifications because such details are provided to ensure confidence [20].

Artificial intelligence and security are confronting with an obligational query, if clarifications about the security procedures in the system were described to people using it (confidence-related clarifications), people then will have the liberty either to proceed operating or not [20]. The value of such notions will gradually increase as smart systems will develop more intelligence [26] [20], and by that time when such systems assemble and manage data about people, even making choices on behalf of them, there must exist a procedure to stay in charge and agree or disagree to what smart systems operate [20].

A rather crucial issue is inquired, that is how systems can be designed in a way that connects social-tech, with software and deliver the required clarifications to be performed by artificial intelligence [20].

B. Contributions in the Field of AI Development

Researchers made quite big and effective contributions in the field of Artificial intelligence that made it more and more convenient and safe to start depending on machine learning even trusting AI with valuable software and information, in this paper we are glad to note some of these contributions made by authors in their 2016 research [27] where they presented a system that evaluate-in-the-circle, where an evaluator's insight is merged to the same level of the machine-learning (ML), to construct an interactive smart system [27].

This interactive smart system is built based on the following structures [27]:

- An analytical environment for a big amount of information about behaviors.
- Collection of techniques for detecting.
- Tool to acquire views and responses from security evaluators.
- An administrated smart model.

The above structures must be implemented in unification with each other non-stop, the system is supported by a true data sets of 3.6 billion record lines, authors thereby stated that the outcomes are proving the system's ability to efficiently protect from unknown attacks [27].

Developing the ability to execute good protection, through the utilization of unsubstantiated ML to spot infrequent or irregular configurations [27]. Though this might activate false-positives warnings, in this case, it'll take an extensive inspection and a lot of operations for them to be terminated [27].

Authors investigated three main threats confronting cybersecurity business, these three they stated might be treated with ML resolutions [27]:

1- Less categorized data.

2- Frequently changing attacks.

3- Low funding, short inspecting time.

To be able to succeed while confronting such threats, there must be actions implanted correctly for each one of them, along with the wise use of evaluators' efforts and time, whether inspecting more new attacks before they make a big impact, shortening the period between inspection moment and termination of the attack, and lowering the frequency of false positives to the lowest point possible [27].

C. AI2

AI2 is an AI-driven predictive cybersecurity platform. The system can be used to detect about 85 % of cyber-attacks. The system first combs through the data and detects suspicious activity. There are different logs that are detected using the behavioral indicators and the system learning that is unsupervised and detect the potential cyberattacks. Then these attacks are presented in front of a user who confirms that actual attack. After the identification from the user, the feedback is incorporated to learn a supervised model. In the next use, the same platform used the supervised model along with the unsupervised model. Again, the feedback is taken from the analyst and the virtual analyst model is again updated. This process is continued again and again, and the system got well incorporated. The detection rate of the unsupervised ML was found to be 7.9 % where with AI2 it was found that 85 % of the attacks were detected which shows a factor of 10x.

It must be considered that the AI2 system achieves a detection rate of 85 % with a low investigative budget of 200 events. This is a tenfold improvement over the unsupervised model that has about a 7.9 % detection rate. If the daily investigative budget is set at about 200 the false positive rate is set at 4.4 %. Moreover, if the investigative budget is increased to about 1000 the unsupervised outlier detection rate was still 73.7% and the false positive rate is > 22% AI2 achieves a rate greater than 86% for the false positive rate of 4.4 % that shows the reduction by the factor of 5.

The system proposed is an interactive learning system, feeding knowledge from what security evaluators of information and accurate comments (figure2):

- An analytical system for big-data: an environment where measurements are performed on behavioral information from multiple objects and perform computation these data
- Collection of detection techniques: This system learns an expressive model of those features derived from the data through unsubstantiated learning, using one of three approaches: solidity, matrix disintegration, or replicator neural networks [27].
- Constant learning: this section includes a constant knowledge feeding by evaluators through an interface [27].
- An administrated smart model: based on evaluators knowledge, the administrated smart model, obtains a model that expects the nature of arriving incidents, either secure or not [27]

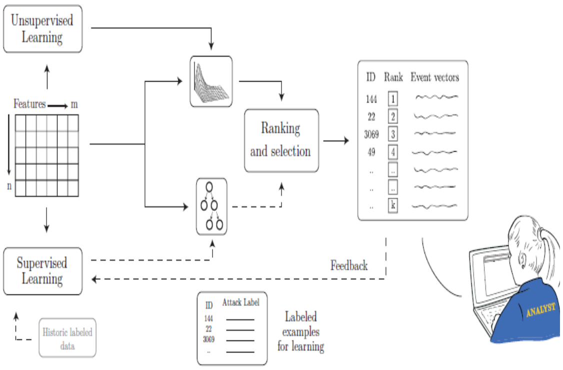

Fig. 1 The interactive smart system [27]

The bid data system or machine is defined as a software infrastructure that is able to ingest data in real-time and develop the quantities that could be easily analyzed either by the machine learning system or the big data systems. A machine learning substrate that sits on top of the system can analyze the data without producing outliers. The provide system incorporates which the analyst feedback generates and use the model continuously that can be trained by the analyst.

4. Conclusion

In this paper, we discussed two of the main components of the cybersecurity infrastructure, the human element, and artificial intelligence. The risks associated with current cybersecurity are taken into consideration and an analysis of the role of AI in future cybersecurity is discussed. A deep analysis of the human factor in the cybersecurity field is done. Different models for recognizing and calculating the variants in the reaction of employees to ISA are discussed. In gender-based analysis, it's determined that older individuals are less likely to be attacked by the vulnerable attacks as compared to people ranging from 18 to 35 years age group. Human behavior to the cybersecurity and it was determined that human behavior to the cybersecurity based on different intentions and results and there are also weaknesses that threaten software security. A deep analysis of machine learning and Artificial intelligence shows that humans have evolved the AI over the course of time and serving different aspects including health, business, and security. Theoretical analysis of the AI is also conducted that shows that AI cybersecurity is delivered through the AI smart systems as opposed to the conventional security system that is delivered by the engineers. However, there is always the requirement for clarifications for all types of cybersecurity systems. There is a lot of contribution of different technologies in the development of AI. At last, an interactive learning system is proposed that uses the data provided.

We went through some details and studies in each element, argued some of the main points of weaknesses and strengths, we aim in future work to upgrade the level of the study on each element, one element at a time using more tools and deep comprehensive research mechanisms. We hope by the writing of this survey to help to describe the full picture of both elements since we believe they represent a strong pair for invincible software security in the future.

References

[1] M. Jouini, L. B. A. Rabai, and A. B. Aissa, "Classification of Security Threats in Information Systems," *ANT/SEIT,* vol. 32, pp. 489-496.

[2] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and information security awareness," *Computers in human behavior,* vol. 69, pp. 151-156.

[3] R. J. Mejias and P. A. Balthazard, "A model of information security awareness for assessing information security risk for emerging technologies," *Journal of Information Privacy and Security,* vol. 10, pp. 160-185.

[4] P. Coopers, "Key findings from the Global State of Information Security Survey 2013," *Changing the game.*

[5] S. M. Furnell, A. Jusoh, and D. Katsabas, "The challenges of understanding and using security: A survey of end-users," *Computers & Security,* vol. 25, pp. 27-35, 2006.

[6] K. Parsons, A. McCormac, M. Butavicius, and L. Ferguson, "Human factors and information security: individual, culture,

and security environment," DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA) COMMANDÂ â€¦.

[7] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)," *Computers & Security,* vol. 42, pp. 165-176.

[8] B. ISO, "iso," *IEC Directives Part,* vol. 1, 2008.

[9] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Computers & security,* vol. 25, pp. 289-296, 2006.

[10] J. HeinstrÃ¶m, "Five personality dimensions and their influence on information behaviour," *Information research,* vol. 9, pp. 9-1, 2003.

[11] M. Pattinson, M. Butavicius, K. Parsons, A. McCormac, and D. Calic, "Factors that influence information security Behavior: An australian web-based study," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 231-241.

[12] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 373-382.

[13] P. E. Spector, "A consideration of the validity and meaning of self-report measures of job conditions," 1992.

[14] C. Vroom and R. Von Solms, "Towards information security behavioural compliance," *Computers & security,* vol. 23, pp. 191-198, 2004.

[15] S. GeriÄ‡ and Å. e. Hutinski, "Information system security threats classifications," *Journal of Information and organizational sciences,* vol. 31, pp. 51-61, 2007.

[16] M. Alhabeeb, A. Almuhaideb, P. D. Le, and B. Srinivasan, "Information security threats classification pyramid," in *2010 IEEE 24th international conference on advanced information networking and applications workshops*, pp. 208-213.

[17] A. McCue, "Beware the insider security threat,â€‹ CIO Jury," 2008.

[18] B.-h. Li, B.-c. Hou, W.-t. Yu, X.-b. Lu, and C.-w. Yang, "Applications of artificial intelligence in intelligent manufacturing: a review," *Frontiers of Information Technology & Electronic Engineering,* vol. 18, pp. 86-96.

[19] Y. Pan, "Heading toward artificial intelligence 2.0. Engineering, 2 (4): 409-413."

[20] W. Pieters, "Explanation and trust: what to tell the user in security and AI?," *Ethics and information technology,* vol. 13, pp. 53-64.

[21] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE transactions on dependable and secure computing,* vol. 1, pp. 11-33, 2004.

[22] B. B. Bederson, B. Lee, R. M. Sherman, P. S. Herrnson, and R. G. Niemi, "Electronic voting system usability issues," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2003, pp. 145-152.

[23] D. Fahrenholtz and A. Bartelt, "Towards a sociological view of trust in computer science," in *Proceedings of the eighth research symposium on emerging electronic markets (RSEEM 01)*, 2001.

[24] B. Harris and D. Allen, Black box voting: Ballot tampering in the 21st century: Talion Pub., 2004.

[25] N. Luhmann, "Familiarity, confidence, trust: Problems and alternatives," *Trust: Making and breaking cooperative relations,* vol. 6, pp. 94-107, 2000.

[26] J. H. Park, "England's controversy over the secret ballot," *Political Science Quarterly,* vol. 46, pp. 51-86, 1931.

[27] K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, and K. Li, "AI^ 2: training a big data machine to defend," in 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), pp. 49-54.

Bayan Al-Amri received her master's degree in cybersecurity studies in 2021. She received her bachelor's degree in Information Technology from Taif in 2013. Bayan's research interests are in cybersecurity, including network security and human behavior.

Hatim Alsuwat is an assistant professor of Computer Science in the College of Computers and Information Systems at Umm Al-Qura University. He received his Ph.D. from the department of Computer Science and Engineering at the University of South Carolina (USC) in 2019. His research interests include Information Security, Cryptography, Model Drift, and Secure Database Systems.

Emad Alsuwat is an assistant professor of computer science in the College of Computers and Information Technology at Taif University. He received his Ph.D. from the department of Computer Science and Engineering at the University of South Carolina (USC) in 2019. His research interests include Probabilistic Graphical Models (esp. Bayesian Networks), Artificial Intelligence, Information Security, and Secure Database Systems.