Chapter

Application of Artificial Intelligence in User Interfaces Design for Cyber Security Threat Modeling

Jide Ebenezer Taiwo Akinsola, Samuel Akinseinde, Olamide Kalesanwo, Moruf Adeagbo, Kayode Oladapo, Ayomikun Awoseyi and Funmilayo Kasali

Abstract

In recent years, Cyber Security threat modeling has been discovered to have the capacity of combatting and mitigating against online threats. In order to minimize the associated risk, these threats need to be modelled with appropriate Intelligent User Interface (IUI) design and consequently the development and evaluation of threat metrics. Artificial Intelligence (AI) has revolutionized every facet of our daily lives and building a responsive Cyber Security Threat Model requires an IUI. The current threat models lack IUI, hence they cannot deliver convenience and efficiency. However, as the User Interface (UI) functionalities and User Experience (UX) continue to increase and deliver more astonishing possibilities, the present threat models lack the predictability capacity thus Machine Learning paradigms must be incorporated. Meanwhile, this deficiency can only be handled through AI-enabled UI that utilizes baseline principles in the design of interfaces for effective Human-Machine Interaction (HMI) with lasting UX. IUI helps developers or designers enhance flexibility, usability, and the relevance of the interaction to improving communication between computer and human. Baseline principles must be applied for developing threat models that will ensure fascinating UI-UX. Application of AI in UI design for Cyber Security Threat Modeling brings about reduction in critical design time and ensures the development of better threat modeling applications and solutions.

Keywords: artificial intelligence, cyber security, human computer interaction, intelligent user interface, machine learning, threat model, user experience, user interface

1. Introduction

Cyber Security protect Information Technology (IT) assets, devices, data, programs, and networks from digital attacks or damage using processes, technologies, and practices to mitigate unauthorized access [1, 2]. Cyber security employs a variety of security concepts such as threat modeling to safeguard user's asset,

environment and organization from being attacked. Threat modeling attempts to enhance cyber security by hypothetically analyzing, itemizing, and prioritizing the potential threats using the attacker's point of view [3]; with an accurate and deep understanding of threats to enable risk evaluation, and subsequently prioritize mitigation against an attack. Neglecting the security designers in cyber security and focusing only on human factors in cyber attacks [4] give room for wide penetration to sensitive systems through social engineering. Consequently, this could pose threats to physical machines and human manipulation via social engineering which is the most important aspect of information security. This ascertains the fact that the issue of cyber attack is progressively becoming a threat that militarizes information technology assets.

Cyber security cuts across technical and social matters and this need to be given priority as there have been a paradigm shift in the movement of businesses and government activities to the online platforms [2]. The complexities and interdependency on the technological system, poses a daunting threat to security engineers as devices and infrastructure are networked in socio-technical environment in which they operate. Therefore, the use of Application Program Interface (API) without the system engineer's control greatly undermines the system properties [5]. This gives rise to the creation of different laws with various provision of Cyber Security data protection, and privacy laws that operates from the inception with over 142 countries [6]. The provision of data protection laws and various security concepts such as threat modeling will be efficiently and effectively put into use if priority is also given to User Experience (UX) through the integration of intelligence in User Interface (UI) design. If UX is seen as having a huge effect on UI design, it could assist security experts in the development of intelligent threat modeling tools that can detect anomalies and make users understand the associated threats in every Human Computer Interaction (HCI).

1.1 Cyber security threat modeling

Threat Modeling (TM) is the basic building block for the establishment of secure systems. Threat modeling is a proactive move towards recognizing potential security concerns and an approach to risk assessment [7]. The success of any cyber security threat model is hinged on the development of an Intelligence System using Artificial Intelligence (AI) paradigms with keen attention on User Interface (UI) that takes into cognizance user interaction. According to [8], particular attention must be paid on what to offer to users as being regarded as a system/tool or an agent/assistant while considering Intelligent User Interface (IUI). IUI must be an Interactive System. Threat modeling must incorporate AI for efficient Human Computer Interaction (HCI) by leveraging on Machine Learning (ML) algorithms to develop a UI with automated capability and improved usability that guarantees high performance. Machine learning algorithm selection for model building can be subjective [9]. Hence, the need for a Multi-Criteria Decision Making (MCDM) approach for optimal algorithm selection [10] is desirable. The threat modeling tools must include components that perceive, learn, interpret, reason and decide; with emphasis on the decision about what is constituted as a threat or not.

Cyber threats lead to risks. Risks in cyber security are as a result of technical vulnerabilities and degradation of fundamental operational practices over time. These practices change organization from safe and sound practices region to a state where an attack will be successful with a greater organizational adverse effect [11]. The security teams investigate threat modeling to assign priority to threats to ensure that attention and resources are spread efficiently. The different levels of priority ensure correct threat mapping resulting from efficient mitigation. Threat modeling often

assist security teams in maintaining safety against possible emerging threats as it is conducted frequently [7]. This frequency can be improved by applying intelligence in the User Interface (UI) design so that the cyber threats can be appropriately modeled using machine learning algorithms. Areas where there is a lack of protection in the adopted tools can also be clarified by modeling threats and facilitating team decision making where the component is appropriate. Krishnan [12] suggested that Intelligent User Interface (IUI) will also be helpful in the prioritization of current applications based on the predicted threat effects and magnitude.

2. Human machine interfaces

Human Machine Interfaces (HMI) deals with the study of two-way transmission of records among users and machines, which establishes a relationship with the user and create user experience [13]. It is natural for individuals to be proud of whatever they produce, no matter how simple it is or complicated as an HMI. Poor HMI designs have been seen as variables contributing to anomalous circumstances and thus exposing the design to cyber security threats. If the principles and practices of HMI are followed, the following are expected to be achieved for the design to be user-centered design:

1. Need to consider the user's aim, obligations with competence

2. Need to consider the mode of processing information by the users and making of decisions.

3. Need to keep the user on top of things and awareness of system condition.

If all these principles and practices are followed, they will improve the cyber security process, but regrettably, various HMIs designs were created with little human input, hence they are technology-centered and are not achieving the desired results. If the aim and the responsibilities of the users are considered with competence, attack threats will reduce. Also, consideration of the user's mode of processing information and decision making must be built into interface design. The successful application of baseline principles leads to trust and the level of trust the users have in a design will govern how they use it. For instance, if a user does not trust a site, he/she will not supply credit card details. If these principles are violated it can lead to credit card hacking. **Table 1** shows the relationship between poor HMI and effective HMI.

Poor HMI	Effective HMI
Piping and Instrumentation Drawing (PID) representation	Layout consistent with operators' model of the process (not a PID)
Presentation of raw data as numbers (temperatures, pressures, etc.)	Depiction of process status and values as information, not numbers
No trends	Key Performance Indicators (KPI) as trends
Bright colors, 3-D shadows	Gray backgrounds, low contrast
Color coding of piping and vessel contents	Consistent visual and color coding
Measurement units in large, bright text	Measurement units in low contrast lettering, if used at all

Table 1.
Characteristics of poor and effective HMI.

Intelligent HMI or HCI can help reduce security problem. A typical example of a security threat in the cyber space is phishing. Many phishing web pages are merely clones of actual sites with minor skewed or masqueraded elements in certain instances. These phishing sites' properties have made Intelligent HMI or HCI problematic for system users as well as several anti-phishing strategies to spot them. Attackers have been able to respond rapidly to anti-phishing initiatives that limits the efficacy of phishing attempts and defend unsuspecting users. Despite the impressive strides made by anti-phishing systems, in recent years, this assault remains one of the most successful. An IUI can be used to reduce the efficacy of phishing attacks and improve consumer understanding of associated threats. Using AI, the interface not only informs the user that there is a phishing attack but also discuss reasons why the website is a phishing site. Such a system is proposed in [14].

2.1 User Interface

User Interface (UI) allows the user to control software applications or hardware devices thus allowing the user have an interaction with the software or hardware of any device especially computing devices. User interfaces are available for both hardware and software devices. A typical example of a hardware device with user interface is the remote control; it has several buttons and sometimes screen to display some basic information. However, the buttons can be used by the user to tell the hardware what to do or what operations to perform. For instance, the use of a keyboard and mouse, each of which has its own user interface, to run a software program. Similarly, through the on-screen menus, a program graphical user interface, can be used to operate a digital camera. According to [15] the aim of a successful user interface, regardless of the program, is to be user-friendly.

UI focus on the looks and styles and it serves as the access point where the user interacts with the designs and system functionalities. UI comes in three forms such as Graphical User Interfaces (GUI), Voice-Controlled User Interfaces (VUI) and Gesture- Based User Interfaces (GbUI) [16]. The GUI allow users to interact with the visual representations of a digital control panel or system. Typical examples are the computer desktops and mobile phone screens. Unlike the GUI, the VUI allow users to interact with the systems and components via voices and speeches. Typical examples are the Google Assistant on Google devices, Siri on IoS devices and Alexa on Amazon devices. The VUI are rampant with more intelligent systems as there is need for a high level of voice recognition and speech processing. For Gesture- Based User Interfaces, the user gets more engaged in the three-dimensional (3-D) space and uses gestures, most especially hand gestures, in interacting with the system. These types of interfaces are mostly used in virtual reality spaces. Three key elements in UI include input control, navigational control and the informational component. Integration of cyber threat related feedback to UI for automated sentiment analysis of the system will aid qualifying potentially new type of attacks or threats.

2.2 User experience

Unlike the UI, that focuses on interfaces, the User Experience (UX) describes and centers on the user's experience of an interaction with the system. Interaction tends to be broader than interfaces as it facilitates dialog and communication between the user and the computing device. The Interfaces are used to experience interactions. Three major dimensions in UX are the users, products and interactions. UX helps to provide a simple way to analyze user product interactions and what influences them. The experience derived from the user product interaction at a given time and

in particular conditions is regarded as UX [17]. It is the individual perception that results from the use or anticipated use of a product/service or system.

UX deals with analysis, experimentation, creation, content, and prototyping, whereas UI is a method of visually leading the consumer through all devices via the interface of a product utilizing interactive elements including cyber threat modeling. To solve a dilemma, UX focuses on all that concerns the user's path during and after the modeling process. UI, on the other hand, is a method that focuses specifically on how the interface of the product look and work. UX is a whole environment that cannot be confined to the screen. On the contrary, UI is typically visual and screen-related content [18]. A deep learning or ML that has the ability to continuously re-train itself based on user activities can be applied to increasing UX in making decision automatically. Example of such is the fake news/hate posts detection model used by some social media platforms.

3. Artificial intelligence in user Interface design

Design focus with Artificial Intelligence paradigms in User Interface is referred to as Intelligent User Interface (IUI) design. AI is revolutionizing industries and changing the status quo, and the design of UI is not left out in its disruption. AI is being used to design tools for providing details to UI designers to aid their designs. AI tools for User Interface (UI) with focus on User Experience (UX) like Uizard and Airbnb's Design AI can turn design sketches into product prototypes [19]. The interfaces must be intelligent enough for adequate detection of cyber threats. An AI-based User Interface threat model will assure reduction in cyber risks. A mainstream example of IUI is the GMail Smart Compose that offers predictive text to complete sentences thus aiding in writing emails faster [20]. An Intelligent Virtual Assistants (IVA) or AI assistant is another example of AI in UI design generally called IUI. Some notable IVA are Amazon Alexa, Microsoft Cortana and ChatBots. Generally, AI can be applied to UI designs on various interfacing channels between human and machines especially when modeling cyber security threats. Channels like search engines (Yahoo search, Google search, Bing, etc) and content recommendation systems (Netflix, Youtube, Spotify, etc) are also significant examples of IUI. Data privacy and considerate integrations, among others are challenges encountered with AI in UI designs, and they must be factored in during the design process for cyber security treat modeling [21]. IUI is aimed at incorporating intelligent automated capabilities and Artificial Intelligence (AI) into Human Computer Interaction. They are human machine interfaces that aims at improving effectiveness and efficiency of Human Computer Interaction (HCI) through the use of reasoning, user models, domains and media such as GUI, VUI and Gesture-Based User Interfaces [22]. IUI sits between AI and HCI. **Figure 1** depicts the relationship between AI and HCI with consideration to IUI.

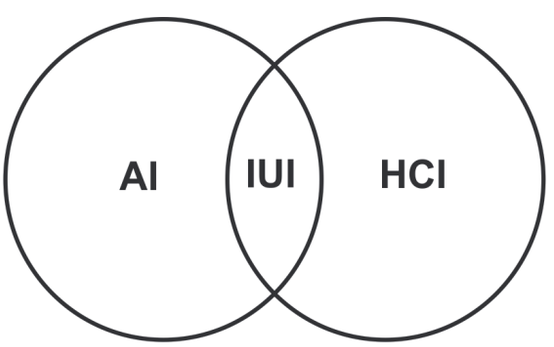

Figure 1.
Relationship between AI, HCI and IUI [23, 24].

HCI provides design techniques for user interfaces that are efficient and the AI components are used to embed intelligence into those interfaces. Basically, IUI is used to depict interfaces that generates some sort of output or exhibits some behavior in which the user interacting with the system considers the system intelligent [25]. A typical example is when a user clicks a wrong button and the interface is able to guide the user on the right button to click. Also, assistance to the user must be readily available through IUI.

Due to diverse models from differing fields that greatly influence user interfaces, the development of IUI is no different, as there are disciplines such as AI which contributes the intelligence in simulation approach to improve responsiveness; software engineering which allows for formal language definition, unified modeling approach, development life cycle; and the Human computer interaction that evaluates the user experience and avails techniques that can be used to create usable user interfaces [26]. In addition to these, there are other fields that still significantly contribute to the development of IUI which is depicted in **Figure 2**.

IUI tends to enhance the interaction between computer and human by bringing about novel approaches of communication and adapting the interface to the user using techniques of AI [27]. The concepts of IUI tend to the intersection of the area of AI and HCI in the field of IUI [28]. This is with a view to automate users' task while engaging in the threat assessment on cyber security [7]. Therefore, the application of intelligence in UI design will in no small measure bringing about better monitoring and controlling of activities that enhance better cyber security measures and threats modeling applications.

The advent of computers which primarily uses a mouse and keyboard as a medium of HCI has brought about a new dimension in the design of UI. This gives rise to the creative and innovative way of UI design for cyber security tools smartly through the use of AI. A new generation of UI which is called IUI keeps rising day by day and improving UX in HCI. IUI attempts the integration of intelligence in HCI that enables the automated capability of UI with the view to improve usability that enables high performance of HCI in cyber security software. It employs design and

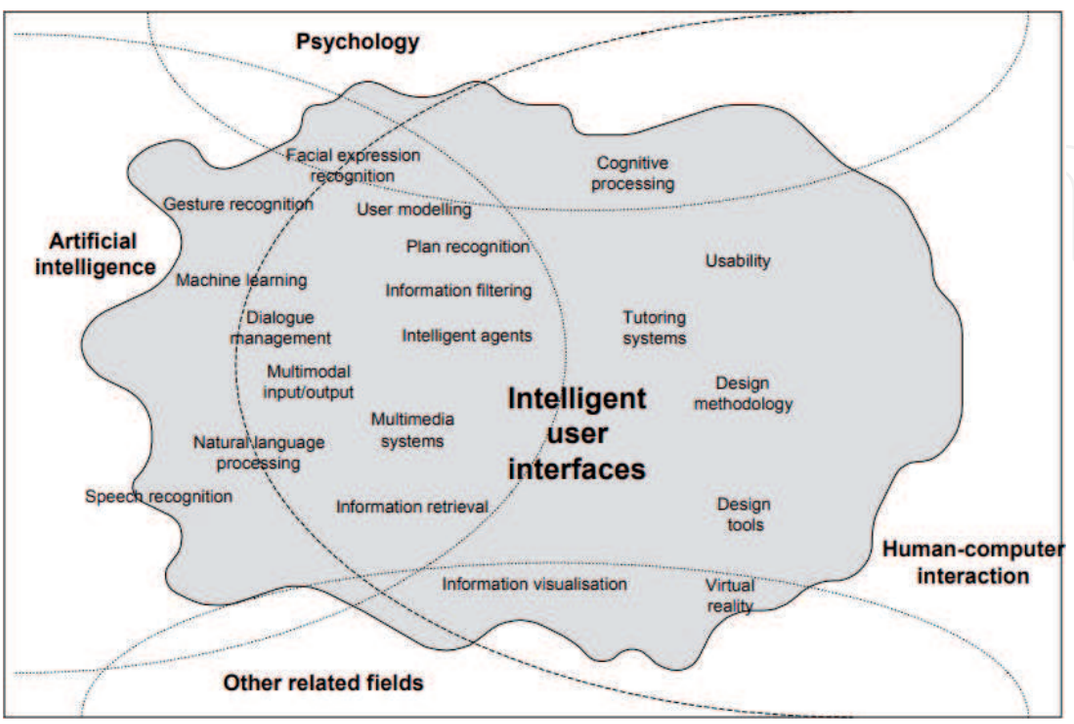

Figure 2.
Research fields of the intelligent user Interface [27].

implementations of AI components that perceive, learn, interpret, reason, and decide with a view to enhancing the capabilities of cyber security experts effectively [24] in decision-making. A different approach and tools can be employed in the implementation of IUI design. The choice of tools and approach is however depending on the goal and the area of application in the cyber security modeling tool. The strong effect of AI on UI/UX is that it helps fix challenges and avails insights and discoveries, however, humans have to recognize the challenges first. AI is therefore less likely to be pre-programmed and more likely to be built with technology so that it can fix the challenges by sustained learning and based on this learning, decisions can be more customized and user-centric. Data can be analyzed and reported in real time with AI.

Applications of machine learning (ML) that communicate directly with daily users are now progressively diverse and ubiquitous. ML is designed to allow a computer to learn about the past or the present and to forecast or predict the knowledge for unknown events in future [29]. The technology's sophistication and prevalence facilitates the belief that AI is the new UX; that is, AI would be the most effective way to boost the user experience [30]. This is because AI will permit UX designers to personalize contents through the application of machine learning algorithms to build intelligent models to mitigate cyber threats.

Typically, the development and design of UI occurs over the following phases as shown in **Figure 3**,

1. On a whiteboard or graphic tablet or even a sheet of tissue paper, designers of the program want to sketch their UI concepts by hand.

2. The designer uses a computer's wireframing method to build the same template again. This is a step that is repetitive.

3. The wireframes are converted into a functioning UI code by UI developers. Before the intended UI is designed, the developers and designers go through an iterative phase. This step is a procedure that is time consuming and tedious.

However, using AI, a handwritten design can be translated to a working UI as shown in **Figure 4**. This code generation usually go through a training phase and a sampling phase. The training phase is where the model is trained to identify images and state the relationships between them using algorithms like the Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) and the sampling phase is more like the prediction phase where samples of UI to be translated will be supplied to the model so as to evaluate and fine tune it's performance.

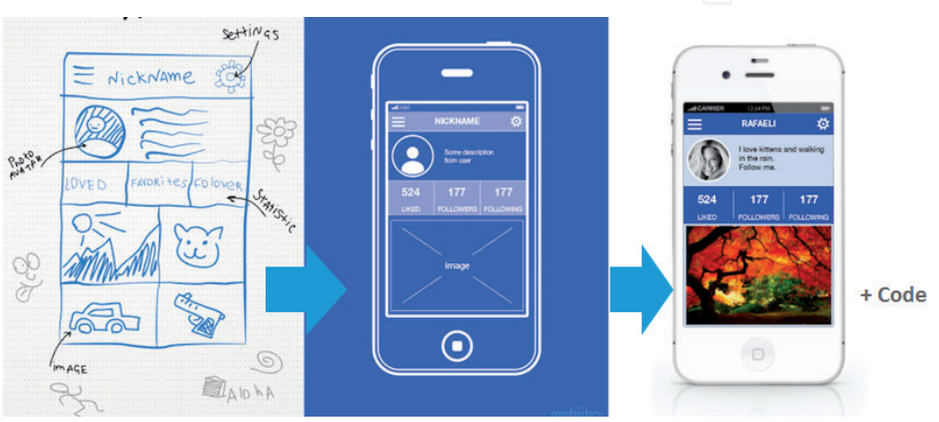

Figure 3.
UI development phases [31].

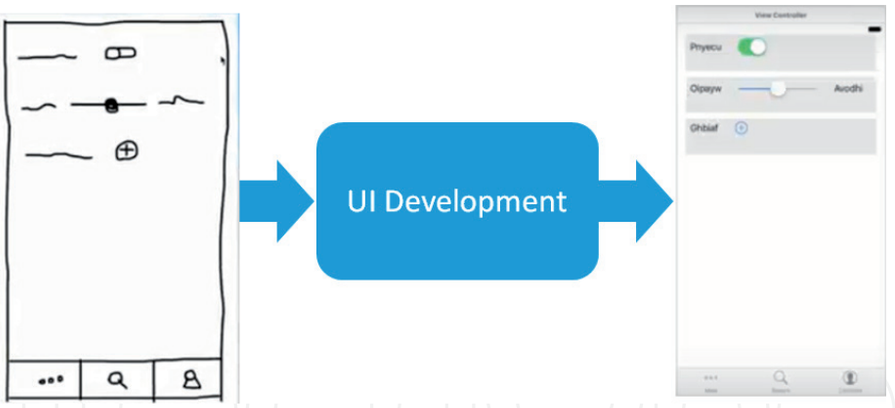

Figure 4.
Translating handwritten design into working UI [31].

The benefits of using AI in the design of UI include but are not limited to:

1. Rapid prototyping, improving iteration cycles, and ultimately better app development for both designers and developers. Critical project time will be saved on design projects when AI-based approach is adopted.

2. It would encourage designers and developers to concentrate on what matters most, adding value to end-users.

3. There will be very little or no barrier in application development as time to learn the use of UI design methods and time to code can be eliminated since everyone can draw UI on paper [31].

4. There is an elaborate interpretation and analysis of data for user-based customizations as vast amount of data can be collected. With AI, on the basis of data interpretation, you get the capacity to configure the interface according to consumer requirements.

5. Real-time learning and seamless adaptation can be achieved using AI in the design on UI. By combining deep learning that uses immense datasets to help draw a conclusion and this helps UI programmers easily build adaptable and improved interfaces.

6. It empowers the interface user. As AI continues to grow, consumers may have the ability to obtain more power over programs, eventually growing confidence and contributing to more usage.

7. It is possible to establish a deep bond with humans as AI systems gather and evaluate a large volume of data, resulting in better relationships.

AI systems can establish a deep bond with humans by creating relationships. Relationships foster where trust grows and this relationship could either be human to human or human to machine. One of the major reasons for the wide adoption of technology (especially AI) is the growing trusts in these systems. This reliance is strengthened by a repeated show of ability in achieving purpose, speed, accuracy, usability, security and privacy amidst other things [32]. By mining enormous data, through the use of deep learning, the trust between AI and humans can be strengthened by the continual generation of useful insights that fits into diverse purposes

and ensure goals are achieved with speed, accuracy and security thereby increasing the usability of such systems. Considering the example of phishing site, the user's trust in the system is bound to increase because the system has protected the user from the phishing attack. Therefore, the user could rely on the AI system to detect phishing sites and help mitigate cyber threats. The more we interact with AI systems, the deeper the connection. For every interaction, data is generated and added to an individual's digital footprint on a system which AI feeds to improve its intellect with humans. AI technologies are also evolving rapidly and currently can analyze human emotions, sparking wild discussions into its unforeseeable future [33].

3.1 Empirical studies on intelligent user interfaces

The complexity and the number of cyber attacks is increasing [34] on a daily basis which poses a lot of threat to both public and private technological assets. Cyber security employ threat modeling techniques in mitigating attacks against technological asset by hackers. Threat modeling allows proactiveness and provides insight to risk evaluation and prioritize mitigation [35]. Formal methods have been found to be profound for performance evaluation compared to traditional methods [36]. As the cyber threat is becoming prominent, application of Artificial Intelligence (AI) in cyber security is another advancement in the technology employed by the experts in the field [34]. The manifestation of AI - enabled UI are Jarvis, Amazon Alexa, Neflix, IBM Watson, Nest Thermostat, Spotify and iRobot Roomba [37]. While advancement in technology to enhance security measure against cyber threat is expedient and important, User Experience (EU) also need to be given a high priority in the User Interface (UI) design to enable high usability and hassle-free workflow. As better security of system should not be tantamount to worse UX, the important factors for enhanced UX and UI in cyber security are balancing the security of system/software with UX, designing of UI based on human perception and minimizing the complexity of software integration into the existing network infrastructure [38]. A poorly designed UI reduces UX which leads to a user performing desired actions with difficulty [39]. An application of AI plays a key role in the IUI to mitigate problems that may arise from human interactions with machine. IUI is regarded as a subset of Human-Computer Interaction (HCI) research with a goal to use smart and current technology to improve HCI.

Applications of AI on UI can drastically improve the interaction between humans and computers. This makes it possible for computers to understand more human communication channels like body gestures, hand gestures, sounds, eye movements, lip-sync and other body motions [40]. This advanced communication with humans via AI has led to innovative solutions addressing human-computer communication barriers. An example is Conversational AI, which is an advanced platform for the widely used online service helpdesk. Conversational AI can analyze an individual's emotion and manage frustrations on the system by routing to different channels for better customer service [41]. With IUI, adaptive, personalized and responsive services can be provided to ensure the specific need of the user is met even when they are yet to realize it. With big data, data mining and deep learning algorithms, technologies that can drive these personalized services could be developed to work in synergy with intelligent environments to mitigate environmental challenges that may arise as a result of human computer interaction.

As the important features of IUI is to enhance the HCI, the following are current techniques used in IUI [27]:

1. **Getting of input from user intelligently:** This involve innovative way of getting user's input through several techniques such as recognition of face

and expression, processing of natural language, recognition and tracking of gesture, and tracking of gaze.

2. **Modeling of User:** This involves all communication techniques that allows the adaptability of human-machine interaction to different environment and users such machine learning, context awareness, among others.

3. **Generation of Explanation:** This covers the entire techniques that enables system explaining its result to users such as IU agents, speech output, feedback of tactile in a virtual environment

The application of intelligence in UI design is to improving users' experience that enables efficiency, effectiveness and user satisfaction using different approaches. This is achieved through the representation of reasoning or acting in accordance to a set of models such as user, dialog, domain, tasks, or speech. As shown in **Figure 5**, different models from different disciplines constitute the development of IUI. AI contributes the simulation of intelligent techniques to enhance the communication, software engineering- enabled notations, unified processes and formal languages while HCI deals on consideration pertaining to users. These combinations of models allow the creation of techniques that allow usable user interface.

IUI applies AI techniques to different input and output with a view to improving UX intelligently. This is achieved through reasoning, representation of knowledge, machine learning, adaptation, and adaptivity as exemplified in various applications such as email filter system, dialog system, email response system and so on [43]. As threat modeling provides answer to questions, "where, what, and how" [3], so also the metrics derive from these questions serve as input and output in AI to improve UX and integrate intelligence in UI designs.

There are two different methods of a user interface that can effectively be applied to intelligence user interfaces in cyber security threat modeling namely direct manipulation and indirect manipulation [7] as depicted in **Table 2**. Also, IUI have been anticipated as a way to overcome a number of the issues that direct manipulation interfaces cannot deal with and further highlighted three principles that can be applicable to threat modeling in cyber security, namely (i) control transparency and predictability (ii) Privacy and trust (iii) treating systems as fellow beings [47].

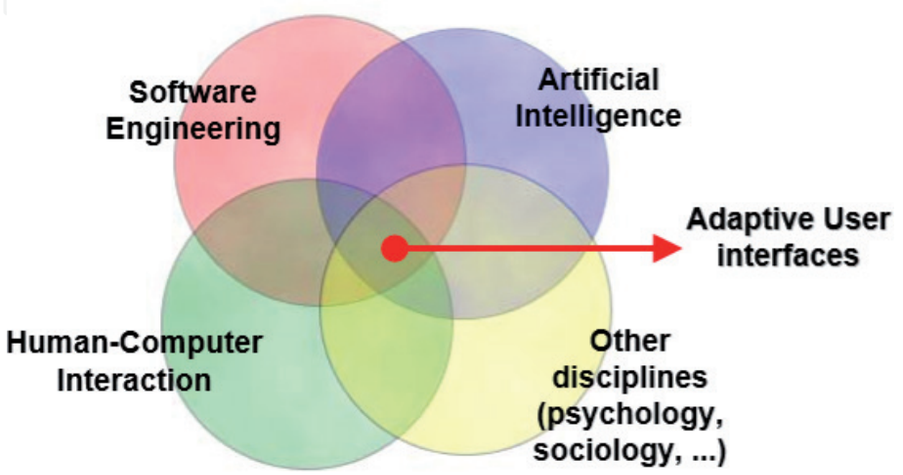

Figure 5.
Disciplines involved In the development of IUI [42].

IUI Design Analysis	Direct Manipulation	Indirect manipulation
Intelligibility: Supports the users to understand the interface action	High	Low
Predictability: Accuracy of algorithm	Low	High
Usability: For evaluating intelligence	High	High
Adaptation: Provision of intelligence in an interface	High	Low

[7, 27, 44–46].

Table 2.
Comparative analysis of IUI.

Ehlert [27] also highlighted a number of issues that recent direct manipulations interfaces will not be able to handle for instance creation of tailored systems, filtering problems, provision of assistance on the use of complex and new programs, taking up the responsibilities from the users with other forms of interaction. The characteristics for developing intelligence in user interfaces designs that enhance the development of a threat model in cyber security are:

1. **Intelligent UI assist the user**: Assisting the user is most often seen as the key action that the intelligent entity performs.

2. **Intelligent UI adapt to the user and automate tasks**: Adaptation, automation, and interaction are the most well-known perspectives that specialists feature while portraying something as intelligent.

3. **Different UI concepts are intelligent in different ways**: Interfaces, systems, agents, and assistants are the most common entities to which researchers attribute intelligence [48].

3.2 Challenges in IUI

Lieberman [49] highlighted the following challenges about IUI for threat modeling in cyber security:

1. failure to give exceptional consideration to transparency and explanation.

2. evaluation of AI interfaces is challenging.

3. invest more in long-term interactions than the predictable interfaces.

4. self-mindfulness and appearance in projects have been a challenge

5. that predictability is not the solitary determinant of usability

Adaption of UI is a challenge for imparting intelligence which comprises the interpretation of user's events and correct prediction of the objectives. In addition, it is a common trade-off, deciding whether to use an easy approach so as to assist functionality. Finally, listed are the three major challenges:

1. Presentation (Human Computer Interaction stage of IUI),

2. Competence (focuses on Artificial Intelligence approaches or procedures)

3. Trust (on the IUI)

3.3 Comparative analysis of intelligent user interfaces

Intelligibility, predictability, usability and adaptation are four characteristics that must be consider while considering User Experience in the design of IUI as shown in **Table 2**.

The Intelligibility of IUI as it relates to how the users understand the interface actions was high when it comes to direct manipulation and low in indirect manipulation. This gives a better understanding of how and when intelligence can substantially improve the design practice (interaction) in the application of cyber security for threat model [47]. On the accuracy of algorithm which explain the predictability, there are many algorithms such as Dynamic Bayesian Network and Naïve Bayes can be used for user's prediction and techniques such as adaptation techniques that provide intelligence for enhancing the predictability of the UI and creating a lasting UX. The performance of these techniques decrease when the accuracy of algorithm by the system becomes low [44]. The usability principles for evaluating Intelligent User Interfaces (rather than direct manipulation systems) ensures that it does not mislead the user's expectation [48]. The provision of intelligence in a UI is highly reliable and cost efficient in direct manipulation than indirect manipulation as the authoring tool enable easy development and maintenance of the intelligent parts of the system [50] especially when it concerns threat modeling due to consideration for various risk metrics.

3.4 IUI design methods

A poorly designed interface can bring about inconvenience to its users. Just like every other product, IUIs need to be built carefully. The need for an IUI should be obvious from the analysis of the issue, instead of making an IUI simply because it is good. First of all, it should be determined whether a device needs an IUI or not because IUIs are typically more computer-intensive than conventional user interfaces. With a user interface, if the same performance can be achieved, why bother making a more complicated and expensive IUI? The final decision whether to build an adaptive process in interfaces or not lies in weighing the expense of deployment against the enhancement of user engagement [51]. If adaptive functionality is introduced in IUIs, the cognitive processing expected by the user will be reduced whereas, installation and management of an IUI would take time and computing resources. In designing IUIs, the following iterative refining steps below are used.

1. **Users, application, and environment review**: In every design process, the review and analysis stage is probably the most critical phase, but much more so in IUI design. There is need to analyze the typical system user, what roles the system is to play, and what method can execute in the design phase of a regular non-intelligent interface. Ideally, an IUI should be able to adjust to any consumer in any environment.

2. **Creation and installation of (prototype) interface methods:** The method of designing innovative strategies and metaphors for interaction is principally

one of imagination. Only getting out and seeking out fresh things and theories is the safest approach however, there are general interface architecture standards. IUI do not necessarily obey the general UI rules for example, user control, access power and consistency [52]. Other criteria, on the other hand, are best suited by IUI than by UI. The usage of natural language in IUI, for example, IUIs will speak the language of the user even more than conventional frameworks of UIs.

3. **Evaluation of the framework which was developed:** The criteria drawn up in the evaluation process should be complied and the feasibility of the prototype device should be studied while usability tests should be defined to assess this quality. These measures may include the number of errors, the completion time of the task, the user's interface attitude, etc. User satisfaction is a very significant but subjective usability criterion [52]. Since the consumer has to interact with the interface, there is need to know whether the design is nice and friendly to work with.

4. **Based on the evaluation results, corrections are made:** A range of concept changes would be made to the existing version depending on the issues found in the evaluation stage. A new round of design, execution, and assessment would then be initiated. Until the outcome is satisfactory, this iterative method will continue. The final interface methodology may be implemented into current user interface design tools if seen to be effective.

5. **Edit the tools for Designing interfaces:** There may also be a fifth stage in the design process, which is concerned with editing the tools for designing interfaces to add a modern approach or metaphor.

The following are some of the design approaches to the application of IUI for better user experience. **Table 3** shows the descriptions of various IUI design methods [53].

Design Methods	Description
Probability-driven State-charts	It uses state-charts to analysis users flow through different states. It creates a probability metrics of users expected actions with various features or events on an interface. This metrics then feed decisions on how the UI is personalized.
Decision Trees	This method utilizes contextual data to determine the choices of user groups. This analysis helps to make intelligent decisions on how different users interacts with a UI.
Prediction via shortest path algorithms	This approach uses weights to determine paths users will frequently take. Its process involves tracking the previous or source state, the next or target state, current event and time of the event to determine user's shortest paths.
Higher-order Markov model	This approach analysis multiple user transitions to predict user's decision on the next path to take. This analysis is focused on users previous or source paths and goes beyond the user's last path to its extended source paths to a destination.
Deep Reinforcement Learning (DRL)	This design approach does an extended prediction into expected user activities. DRL analysis itself towards the predictions of user's behaviors and it either regards itself if the predictions are correct or get punished if otherwise. This learning is done over-time to improve itself towards becoming a perfect user prototype with knowledge of expected actions.

Table 3.
IUI design methods.

3.5 AI versus UI design

The distinguishing factor between the traditional UI design and IUI design is the application of AI for better User Experience (UX). AI introduces a raw ability towards creating individualized interfaces through insights and discovery from understanding users' actions [54]. The user's expectations or intended activity on an interface is what AI feeds on to present a better user experience. The traditional UI is still relative to the design, but AI factors the user's interest to give them lasting User Experience (UX). With the traditional search engines, algorithms are rigid and yield similar search results for the same search input from different users, but AI evolves the search engines to generate smarter results tailored to a specific user. Keyboards is another rigid interface being gradually replaced by sensor-based interactions like body gestures, touchless hand gestures and sounds. Affective computing is another AI intervention, it factors human emotions, moods and expressions [55]. It's an emerging technology that enables a UI to understand and respond to human emotions in hopes of changing the rigid form of human interactions with computers.

Pertinent question must be asked when it comes to AI and UI design. What is the importance of AI to the design of User Interface? This question can only be answered with recourse to HCI. Every process in industrial design field of HCI and AI are intertwined from earliest stage in computer development with core relationship as intelligence even as at today [49]. The intelligence ushers in knowledge representation and interaction management with the application of machine learning algorithms in the design of IUI. The emergence of HCI has brought about a lot of innovations which led to technological development propelled by ubiquitous computing [56]. The idea behind HCI is making computers very easy to use and more helpful while AI is modeling human idea and exemplify those ideas into computer. These relationships bring about the creation of IUI with a high degree of usability. Therefore, AI unravels many difficulties being confronted with in User Interface design and answers many questions relating to User Experience. **Table 4** depicts HCI goals in relation to User Interface design and AI.

HCI Goals	User Interface Design	Artificial Intelligence
Collaboration	It gives attention on collaboration among remotely-located users	It unites the imagined joint effort between the user and the computer, as the computer takes a more lively function
User Input	It is more flexible as users can uninhibitedly blend significant level communication and give definite and explicit directions.	It can give a more flexibility to computer systems input.
Adaptation	It studies users and transfer the results at design time to designers and implementors.	It offers the capacity to move part of the loop comments from design time to run time.
Desired Work Practices	It describes the real-world work practices and assure the systems is constant with these practices.	It represents the work practices as workflow descriptions and document content (both procedural and declarative)
User Experience	It helps users to achieve their personal and work tasks and goals.	It gives opportunity to concretely implement the user's ideas directly in working systems.

Table 4.
AI versus UI design.

The application of AI in UI design is mainly a digital practice and will visually guide the user over the product's interface. There is a brighter future for integration of AI into UI, even though there are several AI algorithms with heuristic nature but these solutions (predefined model, making more established communication as less significant than current ones and excessive accuracy) can assist in the threat modeling for cyber security [44].

3.6 IUI design model

IUI design model depicts the representation of the UI and how the UX will be. The selection of design model is very important because this determines what features and services will be available in the user interface. Using a blueprint may be a major boost in the design process [57]. Some models have an overall architectural model that focuses on user modeling, whilst others propose a multi-modal input architectural model. Input is captured and later pre-processed from the keyboard, mouse, microphone, video, or probably some other input unit. Production entails case marking and other input elements that are interesting. The different modalities are fused and measured after each input modality has been evaluated.

Once all the knowledge required is accessible and revised, the framework must settle on the best choice for intervention. This is called adaptation in **Figure 6**, as some types of interface adaptation are typically selected. Assessment and adaptation sometimes take place concurrently using one inference engine for both, rendering the difference between the process of assessment and adaptation not very obvious. It is also important to produce the selected operation, which is achieved in the segment of performance production. Most IUI can be produced with this model or equipped with it. A general IUI model is shown in **Figure 6**.

3.7 AI-based UI and UX prototyping tools

AI is driving simplicity in UI and UX design, and the following are some of the top use cases.

1. **Uizard:** This tool enables for rapid prototyping of sketches. It converts hand-drawn wireframes into application prototype with working code.

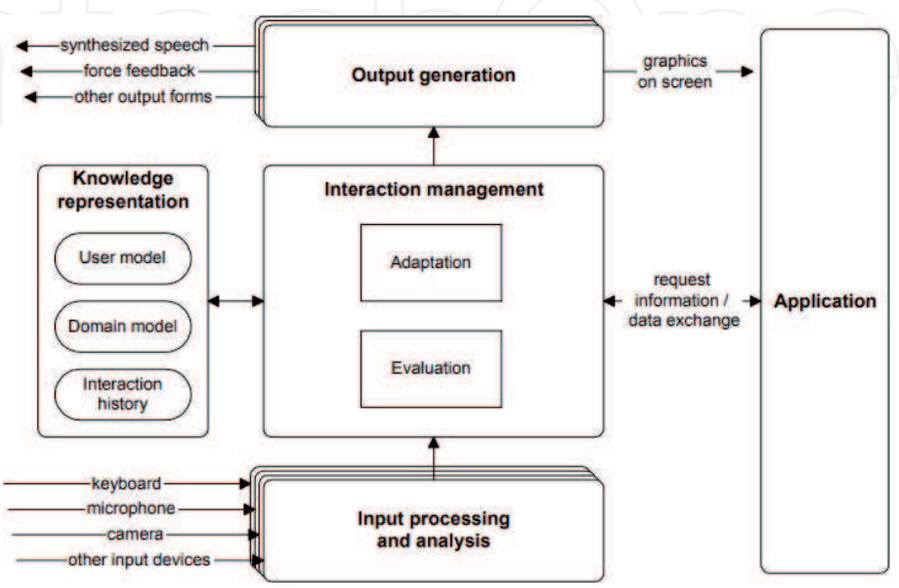

Figure 6.
Intelligent user Interface model [27].

Features	Uizard	Airbnb's Design AI	Mockplus	InVision	Balsamiq
Learning Curve	Minimal	Minimal	Minimal	Minimal	Minimal
Simplicity	High	High	High	Medium	High
Offline capabilities	No	No	No	Yes	Yes
Free to use (No trial)	Yes	No	Yes	Yes	No
Collaboration	No	No	Yes	Yes	Yes
Community Support	Low	Low	Medium	High	Medium
Supported Platforms	Web	Web	Mac / Win	Web	Mac / Win /Web
Code Generation	Yes	Yes	Yes	No	No
In Production	No	No	Yes	Yes	Yes
Developer Specs	Yes	No	No	Yes	No
Screen Transitions	Yes	Yes	Yes	Yes	No
Designs from Scratch	Yes	Yes	Yes	No	Yes
Active Usage	Low	Low	Low	Medium	Low

Table 5.
Comparative analysis of commonly used IUI design tools.

2. **Airbnb's Design AI:** This tool is currently in development and can easily convert design sketches to product prototype with working code.

3. **InVision**: This prototyping tool converts uploaded designs into interactive prototypes.

4. **Mockplus**: This is used for quickly creating interactive prototypes of applications.

5. **Balsamiq Mockups**: This tool easily designs wireframes of applications. The design process and generated wireframes are in sketch format. [58–61]. **Table 5** shows the comparative analysis of commonly used IUI Design Tools.

4. Cyber security threat models

The method of threat modeling is a collection of techniques used to construct a system abstraction, profile possible attacks, goals and procedures, including potential threats index that may occur [62]. A typical threat modeling process includes five components which are threat intelligence, asset identification, mitigation capability, risk assessment and threat mapping. Threat models require the application of Artificial Intelligence for prompt risk reporting. In the second quarter of 2018, the cost of cyber crime damage is projected to hit $6 trillions annually by 2021 and the vulnerabilities of the malware that target machine have been up to 151%. Therefore, Intelligence User Interface (IUI) is desirous for threat modeling. There can be external or internal threats, with catastrophic consequences. Attacks may completely bypass programs or leak confidential information that reduces the customer interest in the system's provider.

There are over a dozen mainstream threat models applied to Cyber Security. Threat models have been in existence since the late 1990s to help fortify cyber security. Meanwhile, [63] noted that irrespective of the availability of various threat models, they all follow five steps. First is a granular breakdown of infrastructure or application, then determining the threats, followed by its preventive measures, next is severity reduction (mitigations) and lastly, ranking of threats [35]. The predictability capacity of the machine learning algorithms is a major factor in threat modeling. There are twelve threat models, but the pioneering model is Microsoft's STRIDE that sprung-off in 1999 and gave rise to subsequent models. STRIDE results in a few false positives and is ideal for teams with little security expertise [64]. Other top models include DREAD, PASTA, LINDDUN, Trike, OCTAVE, CVSS, hTMM, Attack Trees, Persona Non-Grata (PnG), Security Cards, Quantitative TMM and VAST Modeling [65]. An analysis of threat models discovered that hybrid threat models handle more potential attacks than single models [62]. This analysis also recommended the PASTA model because it has a well-structured layout, and its implementation is attributed to sub-systems rather than the whole system. Another threat model worthy of note is the Persona Non-Grata (PnG), tailored to UX design, where users' behaviors and interactions with UIs are analyzed. It outputs a few false positives and it is ideal when the system's weakness is known else it becomes difficult to pinpoint likely threats. The Security Cards model is another endorsement ideal for unusual or advanced attacks and is dependent on brainstorming about possible intrusions. The major drawback of Security Cards is its high false positives [64]. **Table 6** shows the comparative analysis of the features of the most common threat modeling methods that are widely in use.

4.1 Cyber security threat modeling process

Threat modeling involve a number of processes and aspects for efficient mitigation. Failure to include these set of components might lead to incompletion in modeling thereby preventing proper threats prevention. The list of those components is as follows:

4.1.1 Threat analysis

This is called threat intelligence. This has to do with the granular breakdown of infrastructure or application. The section contains information on threat types, affected devices, monitoring mechanism, vulnerability exploitation tools and processes and attackers' motivations. Security analysts also gather and use online sources, proprietary solutions or security communications channels to access information on threat intelligence. This is used to improve the awareness and knowledge on emerging risks to determine the right course of action. Most importantly, it tries to understand the data flow across the system.

4.1.2 Identification of asset

This is called threat determination. Security teams need an in-house inventory of the components and data used, the location of those assets and the security procedures used. This inventory allows security teams to monitor identified vulnerabilities for their assets. It helps to gain insight for asset modifications from an inventory in real-time. For instance, warnings to the possibilities of attacks if assets are introduced, with or without allowed approval. This involves identifying all potential and current threats to the applications/systems.

Features Versus Models	Stride	Pasta	Security Card	Attack Tree	CVSS	QTMM
Documentation	Extremely High Documentation	High Documentation	Less Documentation	Less Documentation	Less Documentation	Extremely High Documentation
Technical Threat Identification	Highly Suitable	Highly Suitable	Highly Suitable	Highly Suitable	Highly Suitable	Highly Suitable
Non-Technical Threat Identification	Highly Suitable	Suitable	Suitable	Highly Suitable	Highly Suitable	Highly Suitable
General Threat Identification	Very Efficient	Very Efficient	Efficient	Moderately efficient	Very Efficient	Very Efficient
Time Consumption	High Time consuming	Extremely time consuming	Moderately time consuming	Moderately time consuming	Moderately time consuming	Moderately time consuming
Usage	Very Easy to Use	Difficult to use	Moderately easy to use	Easy to use	Easy to use	Easy to Use
Model Maturity	High Maturity	Medium Maturity	Low Maturity	Medium Maturity	Medium Maturity	High Maturity
Area of focus	Developer	Attacker / Application	Enterprise	Acceptable Risk	Attacker / Application	All Encompassing
Training / Usage Requirements	Required Less Training	Required More Training	Require Moderate Training	Require Moderate Training	Require Moderate Training	Require Moderate Training
Business Impact	Low	Extremely High	Low	Low	Medium	Medium
Threat Output	Threats properties, system entities, incidents and system limits	Threat management, enumeration, and scoring.	Target out-of-the ordinary threat (sophisticated threats)	System direction and Attack Targets	Scoring System and Severity Ranking	Threats properties, system entities, Scoring System and Severity Ranking
Security Properties	Extremely High	Very High	High	Very High	High	Extremely High
Areas of application	Software Industry and Engineering	Software Industry, Engineering and Banking	Production	Construction and Production	Software Industry and Banking	Software Industry and Project Management

Features Versus Models	**Stride**	**Pasta**	**Security Card**	**Attack Tree**	**CVSS**	**QTMM**
Threat Classification	Very Efficient	Efficient	Moderately Efficient	Efficient	Highly Efficient	Highly Efficient
Stakeholders Input / collaboration	Very High Collaboration	Extremely High Collaboration	Extremely High Collaboration	No Collaboration	No Collaboration	Very High Collaboration
Threat Prioritization	Medium Prioritization and Moderately Efficient	Extremely High Prioritization and Highly Efficient	High Prioritization and More Efficient	Medium Prioritization and Moderately Efficient	Extremely High Prioritization and Highly Efficient	Extremely High Prioritization and Highly Efficient
Reliability	Highly Reliable	Highly Reliable	Extremely Low Reliability	Moderately Reliable	Highly Reliable	Highly Reliable

Table 6.
Comparative analysis of threat modeling methods.

4.1.3 Mitigation capacity

This is called countermeasures. The capability of mitigation (that is, capacity of mitigation) usually apply to technologies for securing, identifying and responding to a particular form of threat but also could mean the security skills, know-how and processes of an enterprise. Assessing the current expertise will help decide whether additional resources are required to minimize a threat. For instance, there could be an initial degree of security against typical malware attacks if there is company-grade Anti-Viruses (AV). To compare the current AV signals with other detection capacities, for example, the security expert can decide if there is a need to invest more. This is centered on preventive measures. This involves analysis of current application cyber attacks, managing the damages done, and fortifying system security.

4.1.4 Evaluation of vulnerability

This is called mitigation or risk assessment. This step addresses identified threats with a focus on high-risk threats. Risk evaluations are related to asset inventories through threat intelligence. These resources are required to help security teams think about their systems' current state and develop vulnerability management strategies. Active device and solution monitoring can also provide risk evaluations. Penetration testing are, for example, effective in checking protection measures. This is to reduce severity.

4.1.5 Mapping of threats

Threat mapping is a method that traces the system's likely path to threats. It seeks to model how assailants can switch from resource to resource and help security teams predict where protections can be implemented or enforced more efficiently. It deals with ranking of threats according to their severity and potential damages to the application.

4.2 Predictive analytics of threat models

Machine Learning (ML) assist in the mathematical models construction which has the ability to explain and showcase complicated behavior without the need for programming [50]. These techniques have a way of improving the HMI in the interface design and further improve the intelligence of the design. The usage of ML in Human Machine Interface/Interaction (HMI) design is not very trivial. Moustakis and Herrmann [66] affirmed that the misperceptions about ML, inadequate familiarity with ML's latent capacity and research shortage are the main sources for declined utilization of ML in HMI design. Though, as of today ML has gained recognitions and advance applications can enhance user capability in UI design which helps in mitigating against cyber security threats. Integration of models that use logs to reactively discriminate transactions based on user' history is essential for cyber security threat modeling.

The challenge usually face during threat analysis is now being fazed away by applying AI coupled with machine learning algorithms, which feeds on data to detect abnormalities in systems. Predictive analysis is AI-driven by data and uses large data to understand malicious activities, identify patterns, and provide insights into potential attacks much quicker [67]. Standardization does not exist, and thus the choice of threat models is deterministic of the project needs like targeted risk area, allocated time, expertise, and stakeholder's involvement [68]. Furthermore,

it is advantageous to apply threat models at the requirement and design stage of the project life-cycle [65] and the use of a well-formulated model for Software Development Life Cycle (SDLC) [69] for efficient threat modeling is desirous. Though AI sheds a positive light on cyber security, it also presents alarming intrusion possibilities for cyber criminals. This ordeal does not limit the impact of AI but rather re-enforces its significance, especially in cyber security threat modeling.

4.3 Baseline principles for intelligent user interfaces design

There are four baseline principles that are essential for designing an AI-enabled User Interface [70].

1. **Management of discovery and expectation**

User expectation is very critical in the design of Intelligent User Interface so that false expectation can be avoided. Thus, the users will know the capability of the tools and its limitation as well as benefits expected with minimal input.

2. **Design to Forgive Mistakes**

The AI is going to make errors. The user interface should be design so that users want to forgive any mistake they encounter from the tools. There should be capacity to understand response from natural language.

3. **Data Transparency and Customization**

There should be transparency in data collection and allow users to customize with vivid dashboard for efficient monitoring. There should be provision for input from the users to alter what AI has learned apart from what has been programmed from the business logic.

4. **Privacy, Security, and User Control**

Security must not be compromised in the design of IUI. Users confidence must be gained by ensuring privacy, security, and the ability for AI control. The user should trust the IUI with their personal data.

4.4 Application of AI in UI design for cyber security threat modeling

Threat Modeling in cyber security assists in examining current and potential vulnerabilities within a system, and has been an instrumental process against security threats [71]. Though favorable, this process has hardly warded off looming security threats that have kept a constant necessity for cyber security improvement, leading to conventional approaches on Threat Modeling. The introduction of AI into UI results in behavioral analysis, which can be applied to the second step of threat modeling called threat determination for forestalling cyber attacks. An effective AI approach tailored to vulnerability management has been on behavioral analysis on an attacker [72].

Threat Modeling incorporates AI to analyze various user interactions with interfaces and detect anomalies for potential attacks. Some software solutions or applications designed to detect cyber threats are Darkrace Immune System, a cyber security platform that uses AI to learn human interaction patterns on system interface for anomaly detection, Vectors' Cognito and Paladion [73]. Codesealer is another software application that provides UI security [74]. Another application is

Automated Virtual Agent for Truth Assessment in Real-Time (AVATAR), a United State government security screening tool designed to detect false information during user interaction with the system and is used for automated interviews at Airport checkpoints [75]. Some of the other applications of AI in cyber security are in the areas of spam filtering and malicious traffic detection. These are cyber threats which requires intelligent models to mitigate the attacks.

It is vital to note that AI has become a valuable tool for cyber criminals, thus reinforcing the significant practice of AI in UI designs [73]. AI application in UI is not left without drawbacks which are generally centred on the lack of pattern-driven dataset, computing and data resources. In addition, the introduction of AI attracts AI-modeled attacks like model evasion, data poisoning and data-stealing, though they can be managed by AI domain expertise with good security practices and safeguards.

5. Conclusion

Cyber security should employ a variety of security concepts such as threat modeling techniques to safeguard asset, environment and organization from being attacked. Five essential components of threat modeling process which are threat intelligence, asset identification, mitigation capability, risk assessment, and threat mapping are pivotal to mitigating security threat that are based on IUI design while taking into cognizance the baseline design principles. There must be proper application of different threat model methods at the requirement and design stages of the project life-cycle using a well-formulated Software Development Life Cycle (SDLC) model. The design of Intelligent User Interfaces requires incorporation of Artificial Intelligence (AI) to analyze various user interactions to detect anomalies such as phishing, spamming, fake news/hate posts, among others. To achieve this, predicative analytics must be institutionalized to further improve the intelligence of the design. Deep leaning can be used for sentimental analysis to determine expressions that can aid in qualifying potentially new type of attacks or threats. AI-driven User Interface (UI) design must be user-centered instead of technology-centered to give lasting UX which cannot be derived or experienced with the traditional UI Design. HCI provides design techniques for User Interfaces that are efficient and the AI components are used to embed intelligence into those interfaces. Therefore, appropriate IUI Design Methods, models coupled with AI-Based UI and UX Prototyping Tools are crucial for developing efficient cyber security threat modeling applications. This is highly essential because in the IUI design, direct manipulation method of design has low predictability which does not guarantee effective cyber threat mitigation.

Author details

Jide Ebenezer Taiwo Akinsola[1*], Samuel Akinseinde[2], Olamide Kalesanwo[3], Moruf Adeagbo[1], Kayode Oladapo[3], Ayomikun Awoseyi[1] and Funmilayo Kasali[4]

1 First Technical University, Ibadan, Nigeria

2 The Amateur Polymath, Lagos, Nigeria

3 Babcock University, Ilisan-Remo, Nigeria

4 Mountain Top University, Ibafo, Nigeria

*Address all correspondence to: akinsolajet@gmail.com

References

[1] DigitalGuardian, "What is Cyber Security ? Definition, Best Practices & More," *DATA PROTECTION 101*, 2020.

[2] M. Veale, I. Brown, and F. Getulio, "Cybersecurity," *J. Internet Regul.*, vol. 9, no. 4, pp. 1-22, 2020, doi: https://doi.org/10.14763/2020.4.1533 Published:

[3] A. Hayes, "A Guide to Easy and Effective Threat Modeling," *Application Security*, 2020. .

[4] Adams A. and Sasse M. A., "U SERS A RE N OT is therefore," *Commun. ACM*, vol. 42, no. 12, pp. 40-46, 1999, doi: doi.org/10.1145/322796.322806.

[5] B. Kostova, S. G.̈urses, and C. Troncoso, "Privacy Engineering Meets Software Engineering.," *On the Challenges of Engineering Privacy By Design*, vol. arXiv:2007. pp. 1-17, 2020, doi: http://arxiv.org/abs/2007.08613.

[6] G. Greenleaf and B. Cottier, "2020 ends a decade of 62 new data privacy laws," 2020.

[7] V. L. Jaquero, F. Montero, J. P. Molina, and P. González, "Intelligent User Interfaces: Past, Present and Future," *Eng. User Interface From Res. to Pract.*, no. September, pp. 1-282, 2009, doi: DOI: 10.1007/978-1-84800-136-7_18.

[8] D. Buschek, "What makes user interfaces intelligent? | by Daniel Buschek | UX Collective," 2020. https://uxdesign.cc/what-makes-user-interfaces-intelligent-9f63b27ca39 (accessed Dec. 26, 2020).

[9] J. E. T. Akinsola, O. Awodele, S. A. Idowu, and S. O. Kuyoro, "SQL Injection Attacks Predictive Analytics Using Supervised Machine Learning Techniques," *Int. J. Comput. Appl. Technol. Res.*, vol. 9, no. 4, pp. 139-149, 2020, doi: 10.7753/ijcatr0904.1004.

[10] J. E. T. Akinsola, O. Awodele, S. O. Kuyoro, and F. A. Kasali, "Performance Evaluation of Supervised Machine Learning Algorithms Using Multi-Criteria Decision Making Techniques," in *International Conference on Information Technology in Education and Development (ITED)*, 2019, pp. 17-34, [Online]. Available: https://ir.tech-u.edu.ng/416/1/Performance Evaluation of Supervised Machine Learning Algorithms Using Multi-Criteria Decision Making %28MCDM%29 Techniques ITED.pdf.

[11] T. R. McEvoy and S. J. Kowalski, "Deriving Cyber Security Risks from Human and Organizational Factors – A Socio-technical Approach," *Complex Syst. Informatics Model. Q.*, vol. 03, no. 18, pp. 47-64, 2019, doi: 10.7250/csimq.2019-18.03.

[12] S. Krishnan, "A Hybrid Approach to Threat Modelling," 2017. doi: 10.13140/RG.2.2.33303.88486.

[13] W. Dong *et al.*, "Soft human–machine interfaces: design, sensing and stimulation," *Int. J. Intell. Robot. Appl.*, vol. 2, no. 3, pp. 313-338, 2018, doi: 10.1007/s41315-018-0060-z.

[14] J. Aneke, C. Ardito, and G. Desolda, "Designing an Intelligent User Interface for Preventing Phishing Attacks," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2020, vol. 11930 LNCS, pp. 97-106, doi: 10.1007/978-3-030-46540-7_10.

[15] P. Christensson, "User Interface Definition," 2020. .

[16] IDF, "User Interface Design," *Interaction Design Foundation (IDF)*, 2020. https://www.interaction-design.org/literature/topics/ui-design (accessed Dec. 20, 2020).

[17] W. Chen *et al.*, "Development and Application of Big Data Platform for Garlic Industry Chain," *Comput. Mater. Contin.*, vol. 58, no. 1, pp. 229-248, 2019, doi: 10.32604/cmc.2019.03743.

[18] Guru99, "UX vs UI: 10 Most Important Differences You Must Know!," 2020. https://www.guru99.com/ui-vs-ux.html.

[19] H. Sarmah, "Top 5 AI-Based Prototyping Tools For UI And UX," 2019. https://analyticsindiamag.com/top-5-ai-based-prototyping-tools-for-ui-and-ux/.

[20] Google, "Use Smart Compose - Computer - Gmail Help," 2020. https://support.google.com/mail/answer/9116836?co=GENIE.Platform=Desktop&hl=en.

[21] S. T. Völkel, C. Schneegass, M. Eiband, and D. Buschek, "What is ' Intelligent ' in Intelligent User Interfaces ? A Meta-Analysis of 25 Years of IUI," in *in Proceedings of the 2020 Conference on Intelligent User Interfaces (IUI'20).*, 2020, pp. 1-20, [Online]. Available: https://arxiv.org/pdf/2003.03158.pdf.

[22] D. Bachmann, F. Weichert, and G. Rinkenauer, "Review of three-dimensional human-computer interaction with focus on the leap motion controller," *Sensors (Switzerland)*, vol. 18, no. 7. MDPI AG, Jul. 2018, doi: 10.3390/s18072194.

[23] V. Potluri, T. Grindeland, J. E. Froehlich, and J. Mankoff, "AI-Assisted UI Design for Blind and Low-Vision Creators," 2019.

[24] D. Sonntag, "Intelligent User Interfaces," in *ISMAR 2015 Tutorial on Intelligent User Interfaces*, 2015, no. May, pp. 1-24, doi: 10.1016/b978-0-08-028572-6.50016-x.

[25] M. Maybury, "Intelligent User Interfaces: An Introduction," 2019.

[26] P. Cybulski and T. Horbinski, "User Experience in Using Graphical User Interfaces of Web Maps," *ISPRS Int. J. Geo-Information*, vol. 9, no. 7, Jul. 2020, doi: 10.3390/ijgi9070412.

[27] P. Ehlert, "Intelligent User Interfaces: Introduction and Survey," 2003.

[28] M. Eiband, S. T. Völkel, D. Buschek, S. Cook, and H. Hussmann, "When People and Algorithms Meet : User-reported Problems in Intelligent Everyday Applications," in *24th International Conference on Intelligent User Interfaces*, 2019, pp. 96-106, doi: 10.1145/3301275. 3302262.

[29] J. E. T. Akinsola, M. A. Adeagbo, and A. A. Awoseyi, "Breast cancer predictive analytics using supervised machine learning techniques," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 6, pp. 3095-3104, 2019, doi: 10.30534/ijatcse/2019/70862019.

[30] K. Carmona, E. Finley, and M. Li, "The Relationship Between User Experience and Machine Learning," *SSRN Electron. J.*, no. 1, pp. 1-11, 2018, doi: 10.2139/ssrn.3173932.

[31] V. Betigiri, "AI based UI Development (AI-UI)," *Medium*, 2018. .

[32] K. Siau and W. Wang, "Building Trust in Artificial Intelligence, Machine Learning, and Robotics," *Cut. Bus. Technol.*, vol. 31, no. 2, pp. 47-53., 2018, [Online]. Available: https://www.cutter.com/sites/default/files/itjournal/2018/cbtj1802.pdf.

[33] K. Darlington, "AI systems dealing with human emotions: how the future will be like with emotional machines," *OpenMind BBVA*, 2018. https://www.bbvaopenmind.com/en/technology/artificial-intelligence/ai-systems-dealing-with-human-emotions/ (accessed Jan. 30, 2021).

[34] EC-Council, "HOW TO USE ARTIFICIAL INTELLIGENCE FOR THREAT INTELLIGENCE," 2020. .

[35] C. Gonzalez, "6 Threat Modeling Methodologies: Prioritize & Mitigate Threats," 2020. https://www.exabeam.com/information-security/threat-modeling/ (accessed Dec. 26, 2020).

[36] J. E. T. Akinsola, A. Kuyoro, M. A. Adeagbo, and A. A. Awoseyi, "Performance Evaluation of Software using Formal Methods," *Glob. J. Comput. Sci. Technol. C Softw. Data Eng.*, vol. 20, no. 1, 2020, [Online]. Available: https://computerresearch.org/index.php/computer/article/view/1930/1914.

[37] S. K. Mandava, "User Interfaces with Artificial Intelligence," *Artificial Intelligence, User Interface, User Experience*, 2020. .

[38] R. Strehlow, "Cyber Security Requires an Important Ingredient," *Strong UX*, 2018. .

[39] H. Jaye, "What Is A User Interface, And What Are The Elements That Comprise one ?," *UI Design*, 2019. .

[40] B. Ganapathy, "How Artificial Intelligence is transforming Human-Computer Interaction, and its implications for Design," *LinkedIn*, 2017. https://www.linkedin.com/pulse/how-artificial-intelligence-transforming-interaction-its-ganapathy/ (accessed Jan. 30, 2021).

[41] S. Kleber, "3 Ways AI Is Getting More Emotional," *Harvard Business Publishing*, 2018. https://hbr.org/2018/07/3-ways-ai-is-getting-more-emotional (accessed Jan. 30, 2021).

[42] M. Redondo, C. Bravo, and M. Ortega, "Intelligent User Interfaces: Past, Present and Future," *Eng. User Interface*, pp. 1-12, 2009, doi: 10.1007/978-1-84800-136-7_18.

[43] D. Sonntag, "Intelligent User Interfaces Design and Implementation," 2016.

[44] R. Tahir, "Analyzing the intelligence in user interfaces," in *SAI Intelligent Systems Conference*, 2015, pp. 674-680, doi: 10.1109/IntelliSys.2015.7361213.

[45] T. G. Gonçalves, K. M. De Oliveira, E. Grislin-Le Strugeon, C. Kolski, and G. H. Travassos, "A systematic literature review on intelligent user interfaces: Preliminary results," in *IHM 2019 - Annexes des Actes de la 31e Conference Francophone sur l'Interaction Homme-Machine*, 2019, pp. 1-8, doi: 10.1145/3366551.3370344.

[46] T. G. Gonçalves and A. R. Cavalcanti da Rocha, "Development process for intelligent user interfaces: An initial approach," 2019, doi: 10.1145/3364641.3364665.

[47] K. Höök, "Steps to take before intelligent user interfaces become real," *Interact. Comput.*, vol. 12, no. 4, pp. 409-426, 2000, doi: 10.1016/S0953-5438(99)00006-5.

[48] S. Shaikh, M. Ajmal, N. Ahmed, and F. Badar, "Comprehensive Understanding of Intelligent User Interfaces," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, pp. 395-401, 2017, doi: 10.14569/ijacsa.2017.080652.

[49] H. Lieberman, "User interface goals, AI opportunities," *AI Mag.*, vol. 30, no. 4, pp. 16-22, 2009, doi: 10.1609/aimag.v30i4.2266.

[50] J. Dudley and P. Kristensson, "A Review of User Interface Design for Interactive Machine Learning," *ACM Trans. Interact. Intell. Syst.*, vol. 1, no. 1, pp. 1-37, 2018.

[51] C. Loitsch, "Designing accessible user interfaces for all by means of adaptive systems," no. May 1982, 2018.

[52] S. Duggirala, "10 Usability Heuristics with Examples," *prototypr.io*, 2016. .

[53] D. Khourshid, "Mind-Reading with Adaptive and Intelligent User Interfaces - YouTube," 2020. https://www.youtube.com/watch?v=adO2crvd3fc&t=805s (accessed Jan. 09, 2021).

[54] Fuselab Creative, "Intelligent Interface User Design. Why It Is Important to Understand The Purpose of IUI |," 2018. https://fuselabcreative.com/intelligent-interface-user-design-when-ai-ui-converge/ (accessed Jan. 09, 2021).

[55] Fuselab Creative, "Intelligent Interface Design–What to Expect in 2019 |," 2019. https://fuselabcreative.com/emerging-trends-in-intelligent-interface-design-what-to-expect-in-2019/ (accessed Jan. 09, 2021).

[56] O. D. Alao, J. V Joshua, and J. E. T. Akinsola, "Human Computer Interaction (HCI) and Smart Home Applications," *IUP J. Inf. Technol.*, vol. 15, no. 3, pp. 7-21, 2019, Accessed: Jan. 02, 2021. [Online]. Available: https://search.proquest.com/openview/70e74bf39099ec671c013b7bf9d9258a/1?pq-origsite=gscholar&cbl=2029987.

[57] H. W. Alomari, V. Ramasamy, J. D. Kiper, and G. Potvin, "A User Interface (UI) and User eXperience (UX) evaluation framework for cyberlearning environments in computer science and software engineering education," *Heliyon*, vol. 6, no. 5, May 2020, doi: 10.1016/j.heliyon.2020.e03917.

[58] UXTOOLS, "Compare Prototyping Tools | UXTools.co - Uxtools.co," 2020. https://uxtools.co/tools/prototyping/ (accessed Jan. 11, 2021).

[59] Keep It Usable, "24 Top UX Prototyping Tools with Downloadable Comparison Table - Learn UX," 2020. https://www.keepitusable.com/blog/top-ux-prototyping-tools/ (accessed Jan. 11, 2021).

[60] S. Ogunsola, "Introduction to Uizard as a Rapid Prototyping Tool | by Soliudeen Ogunsola | Prototypr," *Prototypr*, 2019. https://blog.prototypr.io/introduction-to-uizard-as-a-rapid-prototyping-tool-ab3b6bb8729e (accessed Jan. 11, 2021).

[61] B. Wilkins, "Sketching Interfaces – Airbnb Design," 2020. https://airbnb.design/sketching-interfaces/ (accessed Jan. 11, 2021).

[62] N. Shevchenko, "Threat Modeling: 12 Available Methods," 2018. https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html (accessed Nov. 05, 2020).

[63] J. Fruhlinger, "Threat modeling explained: A process for anticipating cyber attacks | CSO Online," *CSO*, 2020. https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html.

[64] F. Shull, "Cyber Threat Modeling: An Evaluation of Three Methods," 2016. https://insights.sei.cmu.edu/sei_blog/2016/11/cyber-threat-modeling-an-evaluation-of-three-methods.html (accessed Jan. 08, 2021).

[65] N. Shevchenko, B. R. Frye, and C. Woody, "THREAT MODELING: EVALUATION AND RECOMMENDATIONS," 2018. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1083907.pdf.

[66] V. S. Moustakis and J. Herrmann, "Where do machine learning and human-computer interaction meet?," *Appl. Artif. Intell.*, vol. 11, no. 7-8, pp. 595-609, 1997, doi: 10.1080/088395197117948.

[67] S. Blitz, "3 Ways Predictive Analytics Can Boost Your

Cybersecurity," *Sisense Inc.*, 2017. https://www.sisense.com/blog/3-ways-predictive-analytics-can-boost-cybersecurity/ (accessed Jan. 08, 2021).

[68] N. Shevchenko, T. A. Chick, P. O'riordan, T. P. Scanlon, and C. Woody, "THREAT MODELING: A SUMMARY OF AVAILABLE METHODS," 2018. [Online]. Available: https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf.

[69] J. E. T. Akinsola, A. S. Ogunbanwo, O. J. Okesola, I. J. Odun-Ayo, F. D. Ayegbusi, and A. A. Adebiyi, "Comparative Analysis of Software Development Life Cycle Models (SDLC)," vol. 1, pp. 310-322, 2020, doi: 10.1007/978-3-030-51965-0_27.

[70] N. van Esch and F. Heijnen, "Design principles for AI-enabled UI | Deloitte Digital," *Deloitte*, 2020. https://www2.deloitte.com/nl/nl/pages/customer-and-marketing/articles/design-principles-for-ai-enabled-ui.html (accessed Jan. 12, 2021).

[71] LIFARS, "What Is Threat Modeling in Cybersecurity? A Brief Introduction," 2020. https://lifars.com/2020/10/what-is-threat-modeling-in-cybersecurity/.

[72] O. Caspi, "Vulnerability Management: How to Think Like an Attacker," *AT&T Business*, 2021. https://cybersecurity.att.com/resource-center/white-papers/vulnerability-management-think-like-an-attacker (accessed Jan. 08, 2021).

[73] E. Segal, "AI Applications in Cybersecurity with Real-Life Examples," *AltexSoft*, 2020. https://www.altexsoft.com/blog/ai-cybersecurity/ (accessed Jan. 08, 2021).

[74] CodeSealer, "Importance of user Interface protection from cyber attacks - CodeSealer," *Codesealer blog*, 2018. https://codesealer.com/what-is-user-interface-protection/ (accessed Dec. 25, 2020).

[75] L. Christou, "You shouldn't fear an AI lie detector, unless, of course, you have something to hide," *verdict*, 2019. https://www.verdict.co.uk/ai-lie-detector/ (accessed Jan. 30, 2021).