Humanities & Social Sciences Communications

ARTICLE

https://doi.org/10.1057/s41599-023-01673-3 OPEN

Identifying personal physiological data risks to the Internet of Everything: the case of facial data breach risks

Meng Wang[1,2], Yalin Qin[1,2], Jiaojiao Liu[1,2] & Weidong Li[1]✉

Personal physiological data is the digital representation of physical features that identify individuals in the Internet of Everything environment. Such data includes characteristics of uniqueness, identification, replicability, irreversibility of damage, and relevance of information, and this data can be collected, shared, and used in a wide range of applications. As facial recognition technology has become prevalent and smarter over time, facial data associated with critical personal information poses a potential security and privacy risk of being leaked in the Internet of Everything application platform. However, current research has not identified a systematic and effective method for identifying these risks. Thus, in this study, we adopted the fault tree analysis method to identify risks. Based on the risks identified, we then listed intermediate events and basic events according to the causal logic, and drew a complete fault tree diagram of facial data breaches. The study determined that personal factors, data management and supervision absence are the three intermediate events. Furthermore, the lack of laws and regulations and the immaturity of facial recognition technology are the two major basic events leading to facial data breaches. We anticipate that this study will explain the manageability and traceability of personal physiological data during its lifecycle. In addition, this study contributes to an understanding of what risks physiological data faces in order to inform individuals of how to manage their data carefully and to guide management parties on how to formulate robust policies and regulations that can ensure data security.

[1] School of Journalism and Information Communication, Huazhong University of Science and Technology, Wuhan, Hubei Province, China. [2] These authors contributed equally: Meng Wang, Yalin Qin, Jiaojiao Liu. ✉email: liweidong_hust@qq.com

Introduction

We are now on the threshold of a new era of networking in which the Internet of Everything (IoE) can embrace IoE technologies, such as social networking, biometrics, multimedia and data mining, that can build relationships in various ways with terminals, platforms and users by connecting things, people, data and business processes (Adel and Michael, 2014). Given the relentless growth in IoE devices and their interaction with anybody with Internet access, virtually everything from physiological data to behaviour data is collected (Komendantova et al., 2021). The in-depth development of this data offers benefits to society for a variety of purposes in relation to authentication, border security, marketing, photo editing and social networking (Buckley and Hunter, 2011), but it also causes frequent data leakage events due to increased potential for a surveillance society (Buckley and Hunter, 2011).

In the past 5 years, a large number of serious personal data leakage incidents have occurred around the world. For example, in 2019 data leakage from Facebook in the United States impacted 540 million people. In addition, the SenseNets Horizon company leaked billions of facial data. These noncompliant and illegal data processing actions violate data protection laws (Raposo, 2022). Furthermore, in the IoE environment, personal physiological data has the characteristics of uniqueness, forever identification, replicability, irreversibility of damage and relevance of information. Leaked data violates individuals' fundamental rights, such as the right to consent and deletion, privacy, equality and property (Brous et al., 2020; Raposo, 2022; Kindt, 2013). Data leaks can also lead to enormous, permanent damage to governments and enterprises. For example, in 2020 the Clearview AI data breach exposed the firm's client list, resulting in bankruptcy (Hill, 2020).

To prevent data breaches and protect overall privacy, various countries have launched personal data protection mechanisms and promulgated laws and regulations on data security. A total of 142 countries issued data privacy legislation by 2020, of which the General Data Protection Regulation (GDPR) issued by the European Union (EU) has the greatest influence (Greenleaf and Cottier, 2020). Within the EU, the GDPR provides comprehensive and strict protection for facial data, and it gives individuals the right to informed consent and the right to delete. At the same time, countries and companies have also established the ethics compliance review to address accountability and transparency concerns and to mitigate risks. For example, IBM established an Ethics AI Board led by a Chief Privacy Officer for reviewing the ethics of technology rollouts (Almeida et al., 2022).

Although there are numerous efforts to address these concerns, data security and privacy risks have not been eradicated. The IoE era is aimed at connecting everything, and physiological data is easily accessible due to a large number of digital collecting devices around us with high-risk factors for data breaches. Moreover, the complexity of the cloud environment, the abundance of personal data and the lack of a unified framework of risk identification create real challenges to establishing a robust IoE scenario that acknowledges all these elements and comprises comprehensive data regulations (Al-Sharhan et al., 2019; Millard, 2013). Therefore, the identification of personal physiological data risks is the main task of current work and is also an important prerequisite to solve the security and privacy problems of personal physiological data.

Risk identification is the first step of risk management (Ozgur and Alkan, 2020; Mao et al., 2020). Only by choosing an effective risk identification method and correctly identifying personal physiological data risks can we actively take appropriate actions to avoid risks and ensure the safety of personal physiological data. The fault tree analysis method can identify the risks in the fault system and rank the importance of these risks (Ruijters and Stoelinga, 2015). Thus, by collecting, summarising and studying cases of facial data breaches, we can summarise the causes of personal physiological data breaches through the fault tree analysis method and provide insight into personal physiological data security.

The IoE context connecting everything leads to more risk sources for data breaches. Currently, a better and more profound analysis of the data breach risks is necessary due to the lack of an adequate understanding of privacy and risk awareness. Based on these myriad considerations, this study uses facial data breach accidents as the research objects and adopts fault tree analysis to systematically and comprehensively investigate the risks of physiological data breaches in line with the data lifecycle. The paper is structured as follows. The next section provides a literature review of relevant research. In the Methods section, we explain the concepts of fault tree analysis and data lifecycle and further outline the research steps. In the Data and Process section, we describe the data selection criteria and present a complete fault tree diagram of a facial data breach. In the Data Analysis and Results section, we analyse reports of the minimal cut set and reflect on the structural importance of basic events. This work's contributions are presented in the Discussion section, after which the Conclusion section briefly summarises the main findings and implications.

The generation and application of personal physiological data in the era of IoE

The IoE is a massive, complex network ecosystem consisting of various elements such as objects, digital devices, individuals, enterprises, governments and data resources through the support of digital platforms and digital processes (Li, 2020). Compared with the Internet of Things, the IoE has a wider range of connected objects and can interact more profoundly with people and the social environment (Adel and Michael, 2014), while the Internet of Things only connects things (sensors and devices) (Diega and Walden, 2016). In other words, the IoE is based on the Internet of Things but enables 'things' to be connected to any device and anyone using any path (network) and any service at any time (context) and anywhere (Spyros, 2018). In the IoE, the generation and application of personal physiological data mainly occur in the cloud, applications, and terminals.

In the traditional social environment, human's natural attributes essentially belong to the category of privacy and are rarely collected digitally. Nevertheless, personal physiological data has been a crucial resource for data collection in the IoE environment. Physiological data is more reliable and measurable than abstract forms such as behavioural data because physiological data can reflect the human state intuitively and even can capture one's state of mind. In a general sense, all human organs that constitute 'physiological humans' tend to be digitised.

Firstly, especially with the development of Internet of Nano Things (IoNT) technology, more human organs can be digitised and connected to the Internet. As the latest innovation of the IoE, IoNT is a network formed by integrating nanomachines (with a size range of 1–100 nm) with the existing traditional communication network and high-speed Internet (Anand et al., 2017). The IoNT can integrate nanosensors into various miniature objects to realise the intelligent perception of subtle environments, and each of its functional tasks is performed by 'nano machines'. This allows the depth and breadth of the IoE to be greatly expanded and enables sensors to connect nano-scale devices as well. Thus, as long as the nanosensor is integrated into the networked object, it can be connected to and communicate with the Internet (Mainor and Patricia, 2019).

Secondly, the development of face recognition technology and human body recognition technology has allowed increasing amounts of facial data and human body data to be perceived and collected. In order to achieve 'environmental intelligence', the IoE needs to monitor and record the body movements, gestures, location, background and environment of human users (Miraz et al., 2015). Existing face recognition technology is mainly used to distinguish facial attributes. The facial data that can be recognised mainly includes the face frame, the key points of the face, the pose estimation of the face, the natural attributes of the face (i.e., whether one is wearing sunglasses, whether the face is covered, whether there is a beard), and emotional expressions (Kachur et al., 2020). Current human body recognition technology mainly carries out human key point detection, which can accurately estimate the 14 main key points of the human body in pictures or videos, such as elbows, wrists and shoulders (Xu et al., 2021). With multiple scenes, it can estimate multiple postures of standing, sitting and moving so as to detect and recognise postures (Patel et al., 2017).

Moreover, with the innovation of emotion recognition system and emotion computing technology, some new application platforms are trying to scientifically monitor individual emotions (surprised, happy, sad, angry, calm), psychological conditions and ideas by analysing the facial data or voice (Isiaka and Adamu, 2022; Kachur et al., 2020). For example, a mental health platform based on biofeedback and emotional computing attempts to capture and analyse the subtle colour changes of the facial capillaries through the mobile phone camera to achieve the monitoring of instantaneous heart rate and implicit respiration, and on this basis, it helps users resist psychological problems such as tension, anxiety, anger, depression, fatigue and insomnia (Li, 2020). In addition, digital platforms and technology companies integrate and correlate users' physiological data through emotional calculation, in order to summarise the users' emotional response to different stimuli, portray user images, and then put advertisements or carry out targeted promotions (Isiaka and Adamu, 2022).

Finally, with technological progress and the continuous generation of personal physiological data, the application of personal physiological data in medical treatment, finance, education and other fields has expanded rapidly. Taking the medical field as an example, a patient-centred health-data-sharing platform can harvest data from multiple personal digital devices to increase information accessibility and enhance the quality of health services (Dhruva et al., 2020; Al-Sharhan et al., 2019; Carvalho et al., 2019; Haraty et al., 2018; Gagnon et al., 2016). Medical and health wearable devices generally have built-in sensors for measuring human health that can automatically collect important data such as blood pressure, pulse, heart rate and body temperature. At present, smart bracelets, watches, glasses and athletic shoes can all perform this function. Overall, health data is generated from various sources, including electronic medical records, insurance claims, Internet of Things devices, and social media posts, which can be widely shared and applied, especially when it comes to disease treatment (Wang et al., 2017).

Risks to personal physiological data in the IoE

The IoE has a wide range of connected objects and can interact in profound ways with people and the social environment (Mahoney and LeHong, 2012; Adel and Michael, 2014). The IoE has formed a huge user pool and has revolutionised social relations, information and knowledge sharing, as well as marketing opportunities (AlAlwan et al., 2017; Kapoor et al., 2018; Shiau et al., 2017). In this process, a variety of embedded devices or operating systems monitor an individual's vital organs to continuously create physiological data second-by-second in order to provide various intelligent services, such as smartwatches used for evaluating sleeping quality (Sundar, 2020; Kwon et al., 2014). Hence, personal physiological data is becoming the most important data resource in the IoE era, and this data is widely digitised, recorded and tracked.

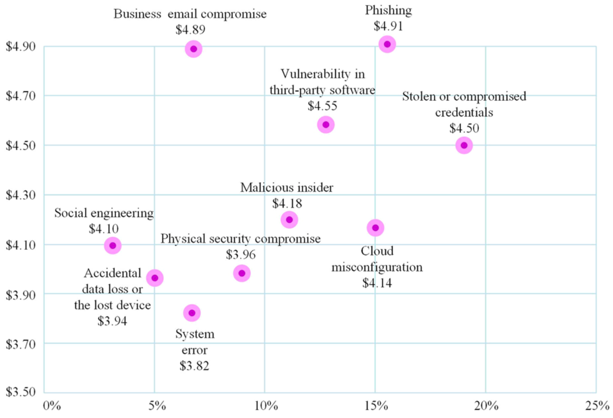


Fig. 1 Cost of a Data Breach Report 2022 (from IBM Security, 2022). Note: Measured in USD millions. The most common initial attack vector in 2022 was stolen or compromised credentials, responsible for 19% of breaches in the study, at an average cost of USD 4.50 million.

However, efficiency and service improvements are often accompanied by increased security concerns (Sundar, 2020; Hadi et al., 2019; Hashem et al., 2016; Hossain and Dwivedi, 2014). Worse still, in the era of the IoE, technology companies, digital media platforms and the government—powered by intelligent collection equipment and information technology—are collecting physiological data on people's digital daily lives in invisible ways. From the security inspection measures in public places such as airports and stadiums to ubiquitous cameras and face payment in supermarkets, physiological data is increasingly becoming an indispensable part of digital life that is almost beyond personal control (Lyon, 2017). A new survey has listed 10 breach risk sources and costs of a personal data breach (see Fig. 1), indicating that data breach is a complex and systematic problem. Particularly, physiological data is sensitive personal data and can face unprecedented threats once leaked (Jain et al., 2008). These threats abound in personal physiological data and may carry dire consequences for individuals, enterprises and nations (Brous et al., 2020). For individuals, physiological data breaches can cause privacy violations, property loss, genetic discrimination, security threats, and serious emotional and mental harm (Chin et al., 2012; Ji et al., 2018; Li et al., 2017; Kindt, 2013; Kilovaty, 2021). Breaches can also violate the fundamental rights of individuals which are enshrined in data protection laws, such as the right to informed consent, access and erasure, which can further damage traditional rights to one's personal image, reputation and dignity. For enterprises, a variety of problems such as reduced credibility, damage to economic interests and lawsuits can result from a data breach (Kshetri, 2014). In the Clearview AI case, several major technology companies such as Google, Facebook, YouTube and Twitter publicly condemned Clearview AI following the data breach. On the national level, the impact of a physiological data breach can be far-reaching. For example, US credit enterprise Equifax was attacked by hackers who breached the data of 143 million US citizens, posing a serious threat to US national security. Undoubtedly, the serious threats of data breaches cause great costs to the damaged entities for mitigating its effect, such as repairing the vulnerability, training employees, legal costs, and more (Kilovaty, 2021), which has led to the urgency of the breach problem. Thus, a better and more profound analysis of the data breach risks is necessary due to the lack of an adequate understanding of threats and risk awareness.

The application and uniqueness of facial data

The GDPR defines personal data as information related to an identified or identifiable natural person (data subject) and limits the processing of special types of personal data (personal sensitive information), including fingerprints, DNA, height, iris patterns, facial features and palm prints. As a special category of personal physiological data, facial data is a highly sensitive form of personal sensitive information. At the same time, facial data has assumed as an increasingly vital role in daily life due to the ubiquitous presence of face recognition technology, which is characterised by high acceptability, collectability and universality (Jain and Ross, 2004; Günther et al., 2017; Sepas-Moghaddam et al., 2019). Face recognition technology became especially successful as a result of the non-contact measures imposed during the COVID-19 pandemic. Scenarios in which face recognition technology has been applied include smart transportation (Karantzoulidis, 2019; Wollerton, 2019; Toor, 2017), device unlocking (Chmielewski, 2015; Finnegan and Kapo, 2018; Tengyuen, 2017), banking (Kan, 2015; Knight, 2017; Petroff, 2016), online retailer services (Association, 2013; Bates, 2017; Pearson, 2018; Romero, 2019), security checks (Wallace, 2018; West, 2019; Wolfe-Robinson, 2019; Oliver, 2019) and health care (Li et al., 2017; Ji et al., 2018).

Compared with other physiological data, facial data is unique. Firstly, facial data can be collected imperceptibly and used widely compared with fingerprint, palmprint or iris data due to non-contact and wide application of face recognition technology, thus facing more breach risks. Secondly, facial data has certain variability. The face can be changed through time, cosmetic surgery or light, resulting in more recognition difficulties and even recognition errors than that of fingerprint, palmprint or iris data. In addition, facial data is a special kind of personal sensitive data related with privacy, which not only covers the personality interests of the ‘face’, such as personal portrait, reputation and human dignity, but also reflects the additional economic value of data. Therefore, due to these similarities and differences, on the one hand, just like facial data breaches, other physiological data breaches can also be caused by similar risk sources and can produce similar serious consequences, such as privacy violations, property loss or physical danger (Sepas-Moghaddam et al., 2019; Ghaffary, 2019; Mehmood and Selwal, 2020; Nandakumar and Jain, 2015). On the other hand, compared with other physiological data, a facial data breach occurs more frequently and can lead to more harmful effects. Given that facial data is widely used and has high breach frequency, it is necessary to study facial data breach risks in order to inform individuals and data management parties of how to manage data carefully. Therefore, the identification of personal physiological data risks, especially facial data risks, is the main task of current work.

Current research on risk identification

Risk identification is the foremost step of risk evaluation and management because timely and effective risk identification serves as the basis of overall safety protection. The results of risk identification can help to inform individuals, government agencies and enterprises of the appropriate measures they should take to address data security concerns. When identifying personal data breach risks, previous scholars have mainly adopted empirical and positive research approaches, and empirical research is more used comparatively. Existing empirical research has identified several risks leading to data breach accidents; these risks are primarily related to IoE devices, IoE technologies, third parties (enterprises, governments), user behaviour, malicious attackers and irregular operations (Palattella et al., 2016; Perlroth, 2016; Kshetri, 2014). Positive research methods are diverse and more often rely on questionnaires. Scholars have used questionnaires to collect information on hidden risks that endanger personal data security and have concluded that insufficient personal protection awareness and imperfect management systems are the reasons for personal information disclosure (Yan et al., 2018; Liu, 2015). As security incidents caused by physiological data breaches have raised concerns all over the world, individuals are increasingly aware of the importance of their physiological data and the possible risks of data breaches (Finnegan and Kapo, 2018). Scholars have also dedicated research efforts to the identification of personal physiological data breach risks (Ratha et al., 2001; Tuyls et al., 2007; Kumar et al., 2018). Previous studies have determined that the risks of physiological data breaches mainly come from indirect attacks and direct attacks (Jain et al., 2018; Smith et al., 2018; Wang et al., 2020). Indirect attacks are carried out from inside the data system, such as attacks by hackers, staff stealing data, template or database modifying, and other unauthorised accessing or activity (Tuyls et al., 2007). Direct attacks mainly refer to technology and device attacks, which are especially prevalent among immature face recognition technology and vulnerable collecting sensors.

In sum, existing research on the risks of personal data breaches has established a basic risk identification reference and listed several risk sources, but the research also has deficiencies. Firstly, particularly in the IoE era, primary data risks arise during data liquidity (Etzioni, 2015; Mayer-Schönberger and Cukier, 2013). To date, there has been little research on risks during data liquidity. Alshammari and Simpson (2017) suggested that understanding the data lifecycle as a representation of data liquidity could be the path to perceiving and tracing physiological data risks. Secondly, few studies have used systematic and objective methods to study and explain personal data breach risks and their logical relationship. A data breach is a kind of accident, but no one has tried to analyse data breaches with accident management methods. Thirdly, physiological data has multiple attributes, once leaked, the consequences are more serious than traditional personal data breaches. Moreover, facial data, as a special kind of personal physiological data, is widely used and has high breach risks. However, there is little research on the identification of personal physiological data breach risks, especially facial data breach risks. Finally, data breach is a widespread and complex problem involving multiple cases, and a single data breach case cannot fully explain comprehensive breach risks, and can no longer meet the research needs.

Methods

There are many studies related to risk identification methods. The main methods of risk identification include fault tree analysis (Yuan et al., 2021), the Delphi method (Gephart et al., 2013), brainstorming (Feng et al., 2017), scenario analysis (Haab et al., 2010), checklist method (Ozgur and Alkan, 2020), Bayesian network analysis (Mao et al., 2020) and the analytic hierarchy process (Liang and Lin, 2017). Considering the complexity of data breaches as well as the effectiveness and reliability of conclusions, we selected fault tree analysis (FTA) as our method for the following reasons.

Firstly, the fault tree analysis method has a wide range of applications and a mature research system. It is a diagram and deductive procedure for safety and reliability analysis in which the causal chain leading to failure is explored using graphical tools (Ruijters and Stoelinga, 2015). It can determine the various combinations of system failures and human errors that can cause undesired events (referred to as top events) at the system level through logic gates (Kabir, 2017). In fault tree analysis, starting from the fault state of the system, we aim to comprehensively identify the risk causes leading to the top event, and we clarify the direct and potential events of the accident through in-depth analysis in a logical and hierarchical way. This method is particularly suited to the analysis of complex systems because it can effectively model a vast number of system components, and it is therefore widely used in the aerospace, energy, network information systems and construction fields.

Secondly, as a massive and complex system, the IoE contains a large amount of personal data. Within such a complex system, there are various factors that can lead to a data breach. Fault tree analysis can be used in complex systems to identify multiple risks caused by personal, administrative and environmental factors in an intuitive and logical way. It can specifically and clearly analyse the causes and propagation processes of faults, which is conducive to further risk management and data safety.

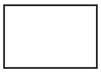
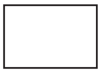
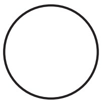
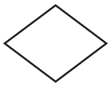
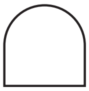
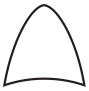
Thirdly, a data breach is a kind of accident, but no one has tried to analyse data breaches with accident management methods. The fault tree analysis method can explore the impact of each basic event on the accident through qualitative analysis so as to determine the priority of measures for the safety control of each basic event and to provide a timely and effective solution or reference for urgent data breach accidents. Therefore, the fault tree analysis method is feasible and appropriate for analysing personal data security problems.

Horton (1985) proposed the concept of an information lifecycle composed of a series of logical stages and maintained that this lifecycle is the natural law of information movement. In the context of information-centric domains, data is dynamic, changeable and ubiquitous, and it is subject to a variety of actions—including collection, storage, usage, transmission and destruction—by several actors for various purposes. These combined actions constitute a data lifecycle. The data lifecycle provides a means to classify, compare and construct data and provides a framework that can systematically and proactively identify and address risks during the various periods of a potential data breach. Likewise, any kind of physiological data undergoes the process of collection, storage, usage, transmission and destruction. In each period of the data lifecycle, a physiological data breach usually involves similar functions, purposes and participants. Therefore, physiological data breach risks can be generalised by taking a facial data breach event as the research object based on data lifecycle.

We regard facial data breaches as an undesired or top event, and we analyse facial data breaches through a case study based on a data lifecycle with five stages: data collection, data storage, data transmission, data usage and data destruction. We adopt fault tree analysis to determine the failure mode leading to facial data breach and the importance of various risk factors to the accident.

The procedure is performed stepwise, with the first step being a choice of the top event (T), in this case, facial data breach, which is an undesirable event associated with the facial data system. The next step is to determine all the secondary events classified into intermediate events (M) and basic events (X) by considering the data lifecycle and risk factors that can cause the top event (T). If two or more secondary events must both occur to cause the top event, these events will be linked in the tree by an 'AND' gate. According to this study, the top event T is caused by the three intermediate events of M_1, M_2 and M_3 with the logic of the 'AND' gate. However, if either of the events will cause the top event, the secondary events will be linked to the top event by an 'OR' gate. Then, an ordering of causative events with a logical relationship will be generated until the fault tree diagram is presented. A further step involves sorting out the minimal cut sets of the fault tree and then calculating the structural importance. Finally, according to the results, we can identify the most significant vulnerabilities in the system and make effective recommendations for reducing the risks associated with those vulnerabilities. The terminologies and symbols in the fault tree diagram are explained in Table 1.

Table 1 Fault tree symbols (Barlow and Proschan, 1975).

Event symbol	Terminology	Description
	Top Event, T represents top event	The TOP event is the accident that is being analysed.
	Intermediate Event, Mi represents intermediate event	The INTERMEDIATE events are system states or occurrences that somehow contribute to the accident.
	Basic Event, Xi represents basic event	The BASIC event indicates a basic initiating event at the limit of resolution.
	Undeveloped Event	The UNDEVELOPED event is undeveloped because there we either lack information or the event is of no consequence.
Gate symbol	Terminology	Description
	AND Gate	The AND gate indicates that the output fault (drawn above the gate) only occurs if two (or more) input faults (drawn below the gate) occur.
	OR Gate	The OR gate indicates that the output fault occurs if at least one of the two (or more) input faults occur.

Data and process. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of or access to personal data (Voigt and Von dem Bussche, 2017). Thus, a breach is more than just losing personal data. Facial data, as a sensitive data type that can be linked to eternal identity, can also have a detrimental impact on an individual or society if the data is breached. In order to identify and enumerate the risks leading to facial data breach and to list the casual events in the fault tree diagram, we collect cases from the China National Knowledge Internet (CNKI) newspaper database, China Search (chinaso.com), Baidu News and Google News using the keywords 'facial data breach', 'facial data accident', 'facial data abuse', 'face recognition' and 'facial data'. We select 22 facial data breach cases that have occurred since 2019 as the research objects. The selected cases meet the following criteria.

1) *Typicality*: The case has attracted extensive attention and discussion across society and has a certain social influence and representativeness.

2) *Availability*: As a method suitable for complex systems, fault tree analysis requires multi-channel and multi-type data to explain and support a case. Therefore, we generally select current cases that have been publicly reported by the media or studied in academic research to obtain detailed supporting materials. These

Table 2 Facial data breach cases.

No.	Case	No.	Case
1	New data breach has exposed millions of fingerprint and facial recognition records	12	Students sue online exam proctoring service Proctor U for biometrics violations following data breach
2	Clearview AI data breach exposes facial recognition firm's client list	13	Hackers breach thousands of security cameras, exposing Tesla, Jails, hospitals
3	In 2019, it was reported that hackers breached Apple's iPhone FaceID user authentication in just 120s	14	The SenseNets Horizon company leaks billions of facial data.
4	A group of hackers breached popular surveillance and facial recognition camera company, Verkada	15	IBM collects online photos without consent, the individual find it impossible to delete their facial data
5	Facial data of thousands of Chinese students has been leaked	16	Everalbum collects facial pictures illegally
6	Residential neighbourhoods across China are adopting facial recognition	17	Facial data leakage of students in some schools in Sichuan and Gansu
7	LLC, transferred copies of CBP's biometric data, such as traveller images, to its own company network	18	Zhang Fu and others violated citizens' personal information and fraud
8	Biometric information exposed in slot machine operator data breach	19	Abuse of face recognition in stores such as Kohler bathroom and BMW
9	7-Eleven breached customer privacy by collecting facial imagery without consent	20	Twinning's personal information breach
10	Consumer-facing companies still have few incentives to stop data breaches, and that's a national security concern	21	The biometric data leakage occurred to Suprema
11	Massive biometric data breach found in system used by banks and Met police	22	Abuse of face recognition technology in housing sales industry (29 administrative punishment cases)

cases have a complete and clear development background, which can ensure the validity of the research.

3) *Heterogeneity*: Facial data breach accidents are pervasive issues, and therefore similar, homogeneous cases that make it difficult to extract variables. As such, cases with a range of fields, places of occurrence and subjects involved shall be considered.

The breach cases are shown in Table 2. The details of these cases can be found in Appendix 1.

This paper analyses and extracts the risks of each facial data breach accident according to two aspects: (1) The causes or risks of facial data breaches are directly pointed out in the news report. For example, in the passenger information breach of U.S. Customs and Border Protection (CBP) in May 2019, the causes for the data breach were that a subcontractor violated the protocol policy and transmitted photos of passengers and license plates to a home network without authorisation; this database was then attacked by hackers. (2) The other aspect is based on the expert analysis of a news report. For example, February 2019 witnessed a facial data breach accident in SenseNets Horizon. The direct causes of the breach were 'no password protection for the internal database' and an 'access restriction configuration fault'. However, some experts added that the company had insufficient security awareness and there are loopholes in its network security compliance.

This paper starts from the top event and then determines the intermediate events, basic events and the logical relationship between them level by level based on the risks of facial data breach cases identified via the aspects of direct cause and expert analysis. Three PhD students initially sort the risks based on the two aspects and then discuss them, and one professor finally checks and confirms the risks. Overall, the validity of the selected cases and collective intelligence contribute to the accuracy and completeness of the identified risks and the logical relationship. After that, to simplify the fault tree diagram, we code each event and present an event code list, as shown in Table 3.

Then, in line with the event code list (Table 3), the events of each level are connected by logic gates according to the logical relationship between the top event (T), intermediate event (M) and basic event (X) sorted from the 22 selected breach cases so as to present the fault tree diagram of facial data breach level by level (as shown in Fig. 2). The first level is the top event (T), the second level is the intermediate event (M), the third level is the basic event (X). Overall, T is caused by M, M is caused by X. T, M and X are all exacted from the 22 cases.

Facial data breach is always caused by various factors. These factors can form some causal chain, such as 'Individual's insufficient security awareness' can be caused by 'Personal greed for small gains' or 'Incautious about the related products' or 'Individuals lack deletion consciousness'. The following example will clearly present how this process could be applied when performing a fault tree analysis on the facial data breach (see Fig. 3):

The event to analyse: M_1 (Risk arisen by individual)

The contributing factor 1: M_4 (Individual's insufficient security awareness)

Possible causes for M_4: X_1 (Personal greed for small gains), X_2 (Incautious about the related products), X_3 (Individuals lack deletion consciousness)

The contributing factor 2: M_5 (Individual's unsafe actions)

Possible contributing factors to M_5: X_4 (Individuals use simple password), X_5 (Individuals upload facial data for entertainment actively and casually), X_6 (Individuals download unapproved APPs)

In this example, factor 1 (M_4) and factor 2 (M_5) combined could ultimately cause M_1, represented by an 'AND' gate, meaning the two events always occur together which could lead to M_1. Each gate is then expanded level by level to ultimately identify the lowest-level causes.

Data analysis and results

Analysis of minimal cut set. In the structural analysis of a fault tree diagram, the minimal cut set (MCS) is the minimal basic event combination leading to the occurrence of a top event, and this reflects the risk of the system. The number of MCSs in the fault tree is equal to the kinds of possibilities leading to the top event. In other words, the more the MCSs, the more the paths of accidents, and therefore the riskier the system. The Fussell-Vesely algorithm is usually adopted to calculate MCSs: starting from the top event, the upper-output event of the logic gate is explained by the lower-input event level by level according to the different logical relations of the intersection. If it is an 'OR' gate, the union of input events (represented by multiplication) is presented. If it is

Table 3 List of events at all levels.

Code	Event	Code	Event
T	Facial data breach	X_{12}	Web crawler collection
M_1	Risk caused by an individual	X_{13}	Illegal collection by offline face recognition camera
M_2	Risk during data management	X_{14}	App illegally opens cameras of mobile phone and other devices to collect data
M_3	Supervision absence	X_{15}	The enterprise has ineffective security measures and insufficient data protection capacity
M_4	Individual's insufficient security awareness	X_{16}	Insufficient safety education
M_5	Individual's unsafe actions	X_{17}	The database without password
M_6	Risk during data collection	X_{18}	Simple username and password
M_7	Risk during data storage	X_{19}	Access rights configuration error
M_8	Risk during data transmission	X_{20}	Incorrectly configured databases
M_9	Risk during data usage	X_{21}	Not desensitised core data
M_{10}	Risk during data destruction	X_{22}	Low server security
M_{11}	The supporting policies not keeping up with technology	X_{23}	Equipment lost
M_{12}	Data is collected randomly	X_{24}	The physically compromised storage device
M_{13}	Insufficient awareness of safety responsibilities	X_{25}	The equipment is not updated in time
M_{14}	Unsafe database	X_{26}	Interface attack
M_{15}	Illegal use	X_{27}	Management account is hijacked
M_{16}	Defective collection equipment	X_{28}	Malware attack
M_{17}	Low difficulty of collection	X_{29}	Data outsourcing, hosted by a third-party company
M_{18}	Illegal collection	X_{30}	Data exiting
M_{19}	Database security protocol flaw	X_{31}	Data is captured during data transmission
M_{20}	Vulnerable physical storage device	X_{32}	Commercial companies actively sell data
M_{21}	Database is attacked	X_{33}	Commercial companies went bankrupt and data was resold
M_{22}	Illegal actions by data management party	X_{34}	Operators steal data
M_{23}	Illegal actions by the third party	X_{35}	Remote access by operators leaves data on other devices
M_{24}	Hacker attack	X_{36}	Illegal storage of data by third parties
X_1	Personal greed for small gains	X_{37}	Illegal transfer of copies by third parties
X_2	Incautious about the related products	X_{38}	The third-party did not delete the data as required
X_3	Individuals lack deletion consciousness	X_{39}	Illegal trade
X_4	Individuals use simple password	X_{40}	The data user has not fully considered or prepared for the risk
X_5	Individuals upload facial data for entertainment actively and casually	X_{41}	The management party failed to delete the data as required
X_6	Individuals download unapproved Apps	X_{42}	Incomplete data deletion
X_7	Immature face recognition technology	X_{43}	Lack of laws and regulations
X_8	The device is invaded by Trojan Horse programme	X_{44}	Lack of collection standards and specifications
X_9	The collection device is invaded physically	X_{45}	Lack of implementation rules for face recognition technology
X_{10}	Rough collection method	X_{46}	The review mechanism of science and technology ethics is incomplete
X_{11}	Concealed collection means	X_{47}	Lack of data deletion mechanism

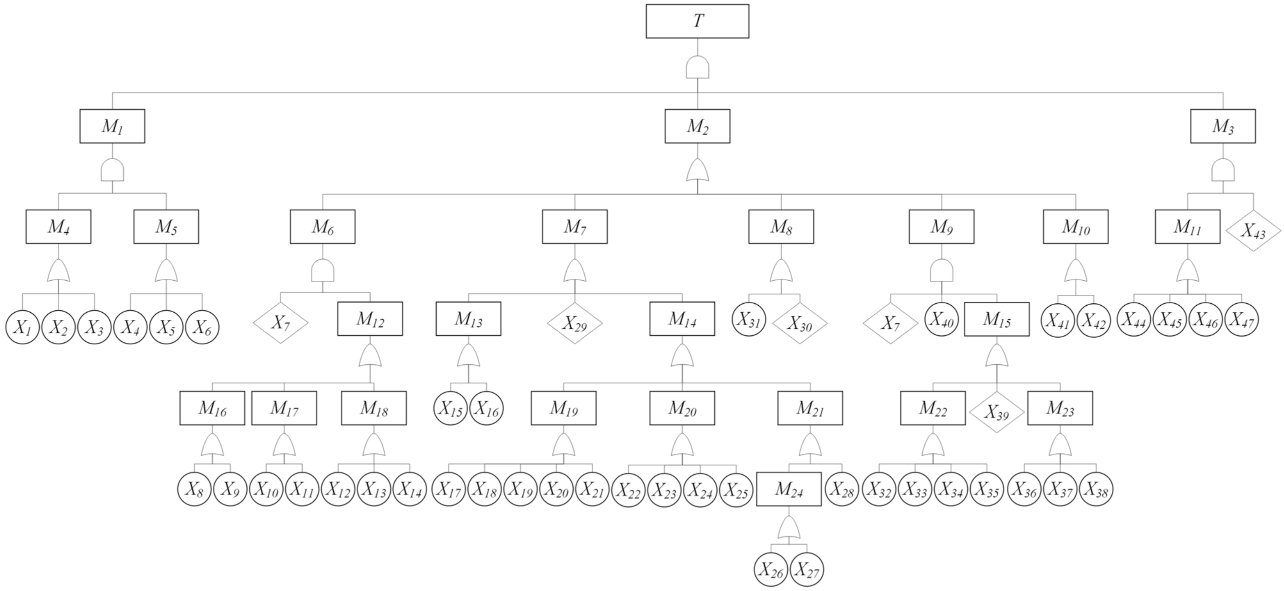


Fig. 2 Fault tree diagram of a facial data breach. T is caused by M, M is caused by X.

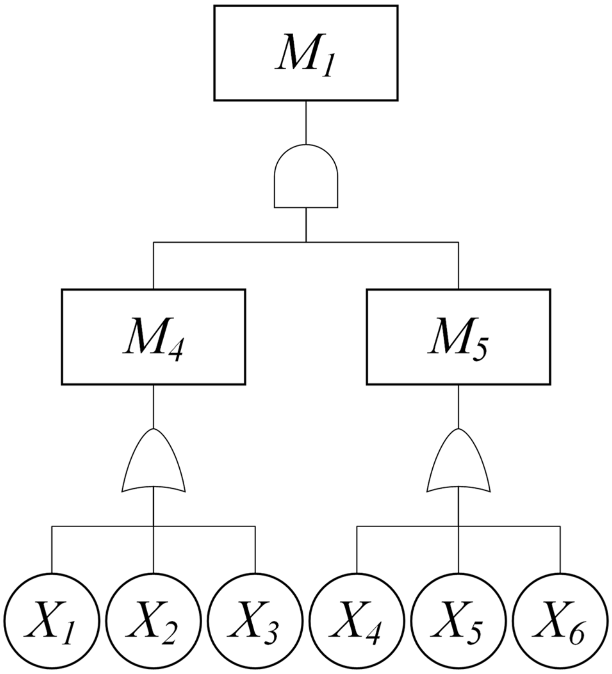


Fig. 3 Part of fault tree diagram of facial data breach. M_1 is caused by M_4 and M_5. M_4 is caused by X_1 or X_2 or X_3. M_5 is caused by X_4 or X_5 or X_6.

an 'AND' gate, the intersection of input events (represented by addition) is presented. This continues until all events are replaced with bottom events (basic events). In this way, the final algorithm result is composed of several MCSs. According to Fig. 1, the top event T is caused by the three intermediate events of M_1, M_2 and M_3 with the logic of the 'AND' gate. In this way, we obtain the formula of the top event as $T = M_1 \times M_2 \times M_3$. Subsequently, M_1 is caused by M_4 'AND' M_5; M_2 is caused by M_6 'OR' M_7 'OR' M_8 'OR' M_9 'OR' M_{10}; and M_3 is caused by M_{11} 'AND' X_{43}.

$$\text{Accordingly, } M_1 = M_4 \times M_5$$

$$\mathrm{M}_2 = M_6 + M_7 + M_8 + M_9 + M_{10}$$

$$M_3 = M_{11} \times X_{43}$$

We simplify the fault tree diagram of facial data breach by Boolean algebra as follows:

$$T = M_1 \times M_2 \times M_3 = (M_4 \times M_5) \times (M_6 + M_7 + M_8 + M_9 + M_{10}) \times (M_{11} \times M_{43})$$

After step-by-step analysis, the bottom combination which cannot be decomposed constitutes the MCS, or the most basic path to the top event. Finally, we obtain 1224 MCSs, indicating that the current facial data system is extremely vulnerable and weak.

Analysis of structural importance. The structural importance analysis serves to assess the importance of each basic event from the fault tree diagram. The occurrence of each basic event has an impact on the top event, but the degree of impact is different. We conduct a structural importance analysis to clarify the degree of impact of each basic event, and we then rank each event according to impact degree. In this way, we can prioritise the events when taking safety precautions and ensure that the system remains economical, effective and safe. As a method of qualitative importance analysis, structural importance analysis is easy to perform and interpret, especially when quantitative data is absent.

There are two means to analysing structural importance: the first is to accurately calculate the structural importance of each basic event and then arrange it from large to small, but this is complex and cannot be carried out when the fault tree is large. The second is to approximately calculate the importance of each basic event according to the MCS. The following four principles should be followed when using the second approach (Barlow and Proschan, 1975):

(1) The structural importance of the basic event in a single MCS is the largest.
(2) All basic events that appear only in the same MCS have the same structural importance.
(3) The degree of structural importance of each basic event that appears in several MCSs with the same number of basic events depends on the number of occurrences; that is, the number of occurrences is low and the structural importance degree is small. The number of occurrences is greater, its structural importance degree is also large. The occurrence times are equal, and the structural importance degree is equal.
(4) If two basic events occur in MCSs with a different number of basic events, their structural importance degree is determined according to the following conditions: ① if their occurrence frequencies in the MCSs are equal, the structural importance degree of basic events in the MCSs with few events is greater. ② If the events appear less often in the MCS with few events and more often in the MCS with multiple events, they can be approximately calculated by the following formula (Zhang and Cui, 2002):

$$\sum^{I}(i) = \sum_{Xi\in Kj} \frac{1}{2^{n_i-1}}$$

where $I(i)$ represents the approximate value of structural importance degree of basic event Xi; $Xi \in Kj$ represents the basic event Xi belongs to the MCS of Kj; and n_i represents the number of basic events in the MCS where the basic event Xi is located.

Based on this principle, the structural importance analysis of the basic event of a facial data breach is carried out. Combined with the fault tree diagram, it is found that X_{43} is a single event that lies at the third level, which is the highest level among all basic events. Therefore, the importance of the basic event X_{43} is the largest. X_7 appears twice in the fourth level of the fault tree diagram. The number of occurrences is higher, and its structural importance degree is accordingly large; therefore, X_7 has the second greatest importance. According to principle (4), if the occurrence frequencies in the MCSs are equal, the structural importance of basic events in the MCSs with few events is greater. Compared with (X_{44}, X_{45}, X_{46}, X_{47}), (X_1, X_2,X_3) and (X_4, X_5, X_6) have fewer basic events, and the importance rank shall be $X_1 = X_2 = X_3 = X_4 = X_5 = X_6 > X_{44} = X_{45} = X_{46} = X_{47}$. Likewise, $X_{44} = X_{45} = X_{46} = X_{47} > X_{40} > X_8 = X_9 = X_{10} = X_{11} = X_{12} = X_{13} = X_{14} = X_{15} = X_{16} = X_{17} = X_{18} = X_{19} = X_{20} = X_{21} = X_{22} = X_{23} = X_{24} = X_{25} = X_{26} = X_{27} = X_{28} = X_{29} = X_{30} = X_{31} = X_{32} = X_{33} = X_{34} = X_{35} = X_{36} = X_{37} = X_{38} = X_{39} = X_{41} = X_{42}$.

Finally, the rank of structural importance of each basic event can be obtained as follows:

$X_{43} > X_7 > X_1 = X_2 = X_3 = X_4 = X_5 = X_6 > X_{44} = X_{45} = X_{46} = X_{47} > X_{40} > X_8 = X_9 = X_{10} = X_{11} = X_{12} = X_{13} = X_{14} = X_{15} = X_{16} = X_{17} = X_{18} = X_{19} = X_{20} = X_{21} = X_{22} = X_{23} = X_{24} = X_{25} = X_{26} = X_{27} = X_{28} = X_{29} = X_{30} = X_{31} = X_{32} = X_{33} = X_{34} = X_{35} = X_{36} = X_{37} = X_{38} = X_{39} = X_{41} = X_{42}$.

By comparing and analysing the occurrence frequency of the basic events in the MCS, it can be found that 'Lack of laws and regulations' (X_{43}) and 'Immaturity of face recognition technology' (X_7) have the greatest structural importance, which are important factors for a facial data breach. Facial data breach is a comprehensive issue involving multiple stakeholders, including technology companies, data platforms and various government departments. At present, it is difficult to clarify and agree on the lack of supervision and which jurisdiction the leakage of facial data belongs to, so it is future critical work to clarify the regulatory authority and regulatory responsibilities as well as to establish a unified and authoritative regulatory body and a multi-sector coordination mechanism. Particularly since the COVID-19 pandemic, face recognition technology has been widely applied, but the technology is far from mature, and there is a lack of corresponding regulatory rules and standards. Considering these vulnerabilities, many countries have issued national technology development strategies and formulated laws, regulations and national standards to monitor the development and application of facial recognition technology. In addition, the events related to individual consciousness (X_1, X_2, X_3) and unsafe behaviour (X_4, X_5, X_6) also have greater structural importance, demonstrating that the individual plays a vital role in personal data protection. Therefore, all related parties should jointly carry out public education on 'Personal greed for small gains' (X_1), being 'Incautious about the related products' (X_2) and the fact that 'Individuals lack deletion consciousness' (X_3) to comprehensively improve individuals' awareness of data protection and further avoid personal unsafe behaviours, such as 'Individuals use simple password' (X_4), 'Individuals upload facial data for entertainment actively and casually' (X_5) and 'Individuals download unapproved apps' (X_6).

Discussion

In this work, we identify potential and traditional breach risks of personal physiological data and assess the degree of importance of risk factors based on the fault tree diagram of facial data breach cases. We are also interested in proposing measures to reduce risks and opening up more avenues for building a robust data system for personal physiological data security.

First of all, the risk sources identified can effectively help identify various risks of physiological data breaches, providing some reference for relevant parties to conduct privacy and data protection. We take facial data breaches as the top event, collect related facial data breach cases, and identify the risks of cases combined with the risk causes of facial data breaches that are directly observed in the news reports and the expert analyses. Based on the risk identification, we list the 24 intermediate events and 47 basic events according to a logical relationship and thus draw a complete fault tree diagram of facial data breaches. According to the fault tree diagram of facial data breaches, we identified 1224 MCSs leading to the top event, demonstrating that facial data is vulnerable and can easily be breached. In the IoE era, personal physiological data is collected, stored and used on a large scale by various Internet service providers, which poses a significant risk of leakage. To some extent, this will seriously threaten the privacy and security of individuals (Li, 2020). Then, through the calculation of the structural importance based on the MCS, we obtained the importance rank of each basic event. The results indicated that 'Lack of laws and regulations' (X_{43}), 'Immature face recognition technology' (X_7), 'Personal greed for small gains' (X_1), 'Incautious about the related products' (X_2), 'Individuals lack deletion consciousness' (X_3), 'Individuals use the simple password' (X_4), 'Individuals upload facial data for entertainment actively and casually' (X_5) and 'Individuals download unapproved apps' (X_6) are the main factors leading to a facial data breach. In addition, in the context of IoE, we have also found some potential breach risk sources that have been ignored by previous studies, such as devices on physical attack surfaces and unsafe data transmission in cloud environments. Aiming at the emerging potential risk sources, the related parties need to update the risk knowledge and take targeted preventive measures to better protect privacy and data security.

Then, we have found that three types of events most easily lead to facial data breach: 'Risk caused by individual' (M_1), 'Risk during data management' (M_2) and 'Supervision absence' (M_3), because they are the three intermediate events closest to the top event. Facial data breach is an integrative problem, and its complexity indicates that a breach is closely related to various factors, such as individuals, data management and legal supervision. Firstly, the disclosure of personal physiological data is closely related to personal active online behaviour. The prevalence of social media and the ubiquity of biometric technology have jointly subverted our way of life (Isaka and Adamu, 2022). Individuals need to use symbols that can identify themselves to promote and show themselves to society. In this process, personal privacy regarded as an important part of digital personal identity will be actively spread. Secondly, data management presents more intensive branches, indicating that data management involves the most breach problems. Primary data is not static and can be changed. Data undergoes a variety of actions for various purposes, including collection, storage, transmission, usage and destruction, which forms the data lifecycle and is difficult to manage. Each data lifecycle model has its own specific focus and risks (Alshammari and Simpson, 2017). Below the data management, the periods of data collection, data storage and data usage are the intermediate events that incur the most risk, indicating that there are many management vulnerabilities in the collection, storage and usage of physiological data. Moreover, a proactive regulator is a significant attribute in privacy security and data protection (Almeida et al., 2022). 'Supervision absence' (M_3) can easily lead to problems such as shifting responsibility, the excessive power of the platform, and difficulties in safeguarding personal rights, which increases the occurrence of data breach events and the severity of risks (Almeida et al., 2022). In recent years, with the popularisation of biometric technology, the supporting regulatory policies and practical operation procedures have not been fully implemented. Although the EU has begun to implement GDPR known as the strictest data act, most countries are still in the exploratory stage. Taking face recognition technology as an example, there are great disputes between several states in the United States and European countries on whether to allow the use of this technology, which reflects the difficulty of legislation and regulation of this technology. Physiological data breach is a comprehensive issue involving multiple stakeholders, including third parties, technology companies, data platforms and various government departments. At present, it is difficult to clarify and agree on the lack of supervision and which jurisdiction the leakage of physiological data belongs to. Overall, the large-scale application of physiological data closely related to personal privacy is a worrying problem. During the data fluid procedure, there are more personnel and processes involved and invisible data breach risks are increased accordingly. Privacy has been placed in the dynamic practice of highly networked social structure, and individuals are increasingly difficult to control the flow and boundary of privacy.

We have assessed the structural importance of each basic event. The basic events are located at the end of each branch of the fault tree, and they are the initial causes of the top event. According to the structural importance of each basic event, it can effectively prevent the occurrence of breach events, timely discover hidden information such as the severity, macro situation, and driving factors of breach events (Ruijters and Stoelinga, 2015), and provide more reliable decision-making support for maintaining the safety of physiological data.

Firstly, we find that 'Lack of laws and regulations' (X_{43}) has the greatest structural importance, which is an important factor for facial data breaches. As individual awareness of data rights is booming, especially due to the COVID-19 pandemic, the formulation of special legislation for personal information protection has become an international demand. Personal information protection rules have been issued all over the world, including the GDPR in the European Union, the California Privacy Rights Act in the US, and the Civil Code and Personal Information Protection Law in China. In 2022, personal information legislation and law enforcement were further promoted, and the proportion of the global population whose personal information is protected will increase from 10% in 2020 to 65% in 2023 (Gartner, 2020). However, the effectiveness of protecting physiological data is unknown due to the absence of specific and unified personal physiological data protection legislation, with some regional laws providing only very basic rights for accountability (Almeida, et al., 2022; Raposo, 2022). Therefore, it is suggested that national agendas should fast-track the process of special data supervision rules, especially focusing on addressing the problems including 'Lack of collection standards and specifications' (X_{44}), 'Lack of implementation rules for face recognition technology' (X_{45}) and 'The review mechanism of science and technology ethics is incomplete' (X_{46}). In addition, special legislation related to personal physiological data protection should also be forward-looking to improve 'The supporting policies not keeping up with technology' (M_{11}). The rapid development of information technology and its profound shaping of society have made data governance increasingly integrated with technology governance. OECD, OECD Digital Economy Outlook 2020 (2020) shows that countries generally recognise that adapting to information technology iteration is the current biggest challenge in data protection legislation and privacy regulations. The data protection laws that apply in the domain of emerging biometric technologies could provide a framework to alleviate individuals' concerns about how their physiological data is used.

Similarly, how to effectively regulate and advance 'Immature face recognition technology' (X_7) has also become a major issue that requires attention. Biometric recognition technology, especially face recognition technology has become widely used in various sectors. It can collect personal data remotely due to its non-contact characteristics, which leads to concerns regarding technical security, personal data disclosure and privacy violation. At present, many platforms publicly refuse to use biometric recognition technology; for example, in November 2021, Facebook claimed it would no longer use facial recognition technology to identify photos. However, the technology itself is not the main problem; if used and developed appropriately, this technology can bring great value to society. Due to the current rapid development of biometric technology, it is complex and highly uncertain, regulation in terms of legislation, government, industry and technology is advisable. In legislation, legal guarantees should be improved to clarify the application boundaries of biometric recognition by setting 'franchise' and entry standards that ensure the security of data information. The government should handle physiological data openly and transparently to ensure the right to access and modify personal physiological data. In terms of industry, the main responsibilities of the industry should be clarified, and the innovation of biometric recognition technology should be encouraged. Regarding the technology itself, the technological protections and technological norms should be strengthened and improved through, for example, encryption protection and authentication. All regulations will contribute to ensuring the security of personal data and promoting the maturity of biometric recognition technology.

Individual errors are the main cause of data breaches and individuals play a vital role in personal data protection (Boxcryptor, 2021). At present, individuals have insufficient awareness of personal privacy protection, they are accustomed to relying on Internet services, and lack an adequate understanding of privacy and awareness of risks. Despite individuals claim the importance of privacy protection, their actual behaviour often belies the importance. Scholars define this gulf between self-reported privacy attitudes and actual privacy behaviours as a privacy paradox (Hargittai and Marwick, 2016). Existing studies mostly explain the privacy paradox based on privacy computing and privacy fatigue (Choi et al., 2018). In the context of the IoE, the risk of personal physiological data breach is usually long-term and hidden, while the immediate interest temptation is direct, individuals usually give up their right to privacy control in order to obtain more personalised services. In addition, faced with complex terms, constantly changing settings and the prevalence of data breaches (Hargittai and Marwick, 2016), feelings of cynicism (Hoffmann et al., 2016), insensitivity (Moritz et al., 2021) or apathy (Hargittai and Marwick, 2016) could make individuals more passive and resigned, and choose not to read or agree directly (Choi et al., 2018). Individuals as the data subject should take the initiative to infiltrate the awareness of maintaining privacy and data security into daily life and reflect on their 'interweaving with social practice' (Seubert and Becker, 2019). Moreover, in the highly connected and networked IoE era, the awareness and ability of individuals to control their personal privacy are compromised by structural violations of privacy. Privacy protection is not an individual process, but rather a collective effect (Hargittai and Marwick, 2016), requiring governments, technology companies, individuals, and other privacy-related participants to continuously adjust policies, regulations, and behaviour patterns in the practice of economic development and technological innovation, in order to achieve privacy protection and comprehensive human development.

Finally, we also found the hidden risk sources of personal physiological data breaches in the IoE terminals and cloud. The IoE terminals are in the perception layer of the IoE, such as smartphones, wearable devices, sensors. Personal data is collected by perception layers in terminals, and then transmitted through the complex network, and finally stored in the server of the cloud service provider. In the context of IoE, the interaction between the IoE terminal devices and the cloud environment will lead to more personal data breach risk sources (Li, 2020; Fosch-Villaronga et al., 2018). First, devices with limited resources are difficult to deploy more advanced security mechanisms (such as complex encryption algorithms) (Iqbal et al., 2016), which can not only be connected by owners but also be intercepted by attackers (Mahmoud et al., 2015). In this case, an attacker can gain access to and control the device and may manipulate or extract data, control or interrupt the service. Second, many terminal devices generally exist in an open, untrusted and unmonitored physical environment, such as traffic control cameras, cloud robotics and environmental sensors exposed to the outside, maybe damaged artificially (Fosch-Villaronga et al., 2018; Iqbal et al., 2016). Third, cloud platforms open personal data to third parties, which also easily leads to personal data breaches. In the future, edge computing or fog computing architecture of 'digital individuals' will be an effective mechanism for data protection in the IoE era (Dang et al., 2019). In this architecture, the terminal device responsible for sensing physical objects sends personal data to the upper layer for processing and storage but does not need to upload all personal data to the cloud in real-time, which to a certain extent allows users to control their personal physiological data independently and reduce personal physiological data breach risks from the source.

Conclusion

In the IoE environment, the emergence of a series of data technologies such as multimedia, biometrics, cloud computing and data mining has opened a new set of possibilities for innovative services and applications. However, this technology also introduces a complex scenario that must be efficiently managed to protect data security. In this scenario, the identification of personal physiological data risks is key to ensuring privacy and data security in the IoE environment. This study provides an important practical approach to revealing the occurrence and evolution mechanism of personal physiological data breaches and to implementing privacy protection measures by taking facial data breaches as a research object. Based on the findings, we maintain that personal physiological data breach has become a key security issue that deserves more attention in the theoretical and practical arenas. Overall, the core contributions and innovations of this research can be summarised into three aspects.

(1) In terms of method, this study firstly attempts to use fault tree analysis to analyse facial data breaches, which is feasible and innovative in method. The security problem of physiological data systems is not caused by one aspect, and there are various relationships between many security risks. However, few studies have used systematic and objective methods to study and explain personal physiological data breach risks and their logical relationship. It is more comprehensive and reasonable to explore the logical relationship between risk sources at a deeper level in combination with real cases and to understand the importance of various factors in the whole risk system to then take well-directed measures.

(2) In terms of practice, the construction of the fault tree diagram of a facial data breach can help the data management parties track the development of the data breach system and provide a knowledge base for risk identification. On the one hand, the knowledge base of risk sources can provide support for the identification of risk sources of subsequent physiological data breaches; On the other hand, the causal relationship is used to clarify the structural characteristics of the accident system, which is convenient for the control of the panoramic situation of physiological data breach and the oversight of the breach risk sensitive nodes. Moreover, it is of practical significance for improving the ability of risk adaptive governance and supporting the manageability and traceability of physiological data from data collection to data destruction.

(3) In terms of theory, this study explores the plight of physiological data in the IoE era, providing a reference for privacy protection under the new situation. This study confirms that in a highly networked environment, a physiological data breach is a systematic process, so privacy protection is not a personal process, but a collective effort. In addition, it is found that the security of physical devices and the complexity of the cloud environment have triggered some new risk sources, providing ideas for building an effective mechanism for personal privacy protection in the future IoE era and enriching the relevant theories of privacy management.

Data availability

The data used in this article has been included in the article.

Received: 25 September 2020; Accepted: 13 April 2023;
Published online: 08 May 2023

Appendix 1 The details of 22 cases

NO.	Time	Case	Risk	Expert analysis	URL
1	2019	New data breach has exposed millions of fingerprint and facial recognition records	Simple user name and password; Access rights configuration error; Data exiting	-	https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/?sh=2f1bbaf546c6
2	2020	Clearview AI data breach exposes facial recognition firm's client list	The hacker; Individuals upload facial data for entertainment actively and casually, which are crawled;	Lack of collection standards and specifications	https://www.cpomagazine.com/cyber-security/clearview-ai-data-breach-exposes-facial-recognition-firms-client-list/
3	2019	In 2019, it was reported that hackers breached Apple's iPhone Face ID user authentication in just 120 seconds	The hacker; Immature face recognition technology	-	https://www.analyticsinsight.net/what-will-happen-when-a-facial-recognition-firm-is-hacked/
4	2021	A group of hackers breached popular surveillance and facial recognition camera company, Verkada	Hacker attack; Illegal collection by offline face recognition camera	-	https://www.analyticsinsight.net/what-will-happen-when-a-facial-recognition-firm-is-hacked/
5	2020	Facial data of thousands of Chinese students has been leaked	Data outsourcing, hosted by a third party company	Lack of laws and regulations; Lack of implementation rules for face recognition technology； Insufficient safety education	https://baijiahao.baidu.com/s?id=1656340231011283716&wfr=spider&for=pc

Table (continued)

NO.	Time	Case	Risk	Expert analysis	URL
6	2020	Residential neighbourhoods across China are adopting facial recognition	Incorrectly configured databases; Insufficient safety education	–	https://www.scmp.com/abacus/tech/article/3104512/facial-recognition-data-leaks-rampant-across-china-covid-19-pushes
7	2019	LLC, transferred copies of CBP's biometric data, such as traveler images, to its own company network	Malware attack; Remote access by operators leaves data on other devices; The improper download and storage of database data	–	https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf
8	2021	Biometric Information Exposed in Slot Machine Operator Data Breach	Malware attack; Illegal storage of data by third parties; Illegal transfer of copies by third parties	–	https://findbiometrics.com/biometric-information-exposed-in-slot-machine-operator-data-breach/
9	2021	7–11 breached customer privacy by collecting facial imagery without consent	Low server security; App illegally opens cameras of mobile phone and other devices to collect data;	Lack of deletion consciousness; Lack of collection standards and specifications	https://www.zdnet.com/article/7-eleven-collected-customer-facial-imagery-during-in-store-surveys-without-consent/
10	2021	Consumer-facing Companies Still Have Few Incentives to Stop Data Breaches, and That's a National Security Concern	Operators steal data	The enterprise has ineffective security measures and insufficient data protection capacity	https://www.cfr.org/blog/consumer-facing-companies-still-have-few-incentives-stop-data-breaches-and-thats-national
11	2019	Massive biometric data breach found in system used by banks and Met police	The database without password; Web crawler collection	The physically collection device is invaded physically	https://www.itpro.co.uk/data-breaches/34206/massive-biometric-data-breach-found-in-system-used-by-banks-and-met-police
12	2021	Students sue online exam proctoring service ProctorU for biometrics violations following data breach	The third-party did not delete the data as required; The review mechanism of science and technology ethics is incomplete; Lack of data deletion mechanism	–	https://lawstreetmedia.com/news/tech/students-sue-online-exam-proctoring-service-proctoru-for-biometrics-violations-following-data-breach/
13	2021	Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals	An international hackerUnauthorized access	–	https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams
14	2019	The SenseNets Horizon company leaks billions of facial data	The database without password ; Individual's insufficient security awareness; Database security protocol flaw	Illegal trade; The enterprise has ineffective security measures and insufficient data protection capacity; The database without password; Access rights configuration error	https://baijiahao.baidu.com/s?id=1625635651342970434&wfr=spider&for=pc
15	2019	IBM collects online photos without consent, the individual find it impossible to delete their facial data	The management failed to delete the data as required Hacker attack	–	https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921
16	2021	Everalbum collects facial pictures illegally	App illegally opens cameras of mobile phone and other devices to collect data; The management failed to delete the data as required	Lack of laws and regulations; Lack of implementation rules for face recognition technology	https://www.latimes.com/business/story/2021-01-29/column-facial-recognition-privacy
17	2020	Facial data leakage of students in some schools in Sichuan and Gansu	Unsafe database; Illegal storage of data by third parties	–	https://baijiahao.baidu.com/s?id=1656340231011283716&wfr=spider&for=pc
18	2020	Zhang Fu and others violated citizens' personal information and fraud	Commercial companies actively sell data; Immature face recognition technology	–	https://www.sohu.com/a/373482018_120032

Table (continued)

NO.	Time	Case	Risk	Expert analysis	URL
19	2021	Abuse of face recognition in stores such as Kohler bathroom and BMW	Concealed collection means; Rough collection method; Illegal trade	Lack of laws and regulations; Lack of implementation rules for face recognition technology	https://www.sohu.com/a/456089454_393779
20	2019	Twinning's personal information breach	Incautious about the related products; Incorrectly configured databases; The physically invaded collection device	-	http://www.woshipm.com/ai/1844718.html
21	2019	The biometric data leakage occurred to Suprema	Not desensitized core data; Data deletion incompletely; The physically compromised storage device	Commercial companies went bankrupt and data were resold	https://us.norton.com/internetsecurity-emerging-threats-biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data.html
22	2020	Abuse of face recognition technology in housing sales industry (29 Administrative Punishment Cases)	Concealed collection means; Illegal transfer of copies by third parties	Lack of implementation rules for face recognition technology; The review mechanism of science and technology ethics is incomplete	https://m.thepaper.cn/baijiahao_10148531

References

Adel SE, Michael ML (2014) Cyber security challenges in Smart Cities: safety, security and privacy. J Adv Res 5(4):491–497. https://doi.org/10.1016/j.jare.2014.02.006

AlAlwan A, Rana NP, Dwivedi YK, Algharabat R (2017) Social media in marketing: a review and analysis of the existing literature. Telemat Inform 34(7):1177–1190. https://doi.org/10.1016/j.tele.2017.05.008

Almeida D, Shmarko K, Lomas E (2022) The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI Eth 2(3):377–387. https://doi.org/10.1007/s43681-021-00077-w

Alshammari M, Simpson A (2017) A UML profile for privacy-aware data lifecycle models. In: Computer Security: ESORICS 2017 international workshops, CyberICPS 2017 and SECPRE 2017, Oslo, Norway, September 14–15, 2017, Revised selected papers 3. Springer International Publishing, pp. 189–209

Al-Sharhan S, Omran E, Lari K (2019) An integrated holistic model for an eHealth system: a national implementation approach and a new cloud-based security model. Int J Inform Manage 47:121–130. https://doi.org/10.1016/j.ijinfomgt.2018.12.009

Anand N, Vikram P, Dac-Nhuong L (2017) Internet of Nano Things (IoNT), next evolutionary step in nanotechnology. Nanosci Nanotechnol 7(1):4–8. https://doi.org/10.5923/j.nn.20170701.02

Association P (2013) Tesco's plan to tailor adverts via facial recognition stokes privacy fears. Guardian. http://www.theguardian.com/business/2013/nov/03/privacy-tesco-scan-customers-faces. Accessed 25 Dec 2022

Barlow RE, Proschan F (1975) Importance of system components and fault tree events. Stoch Proc Appl 3(2):153–173. https://doi.org/10.1016/0304-4149(75)90013-7

Bates D (2017) Face recognition technology set to transform retail. FORBES. https://www.forbes.com/sites/sap/2017/11/08/face-recognition-technology-set-to-transform-retail/. Accessed 20 Feb 2021

Boxcryptor (2021) Human errors are still the top cause of data breach-interview with Paula Januszkiewicz, Expert of cyber security. Inf Secur Commun Priv 12:36–39

Brous P, Janssen M, Herder P (2020) The dual effects of the Internet of Things (IoT): a systematic review of the benefits and risks of IoT adoption by organizations. Int J Inf Manage 51:101952. https://doi.org/10.1016/j.ijinfomgt.2019.05.008

Buckley B, Hunter M (2011) Say cheese! Privacy and facial recognition. Comput Law Secur Rev 27(6):637–640. https://doi.org/10.1016/j.clsr.2011.09.011

Carvalho JV, Rocha Á, Vasconcelos J, Abreu A (2019) A health data analytics maturity model for hospitals information systems. Int J Inf Manage 46:278–285. https://doi.org/10.1016/j.ijinfomgt.2018.07.001

Chin CA, Crosby GV, Ghosh T, Murimi R (2012) Advances and challenges of wireless body area networks for healthcare applications. In: 2012 International Conference on Computing, Networking and Communications (ICNC). IEEE, pp. 99–103

Chmielewski D (2015) Apple to use selfies to unlock phones? Vox. https://www.vox.com/2015/3/31/11560978/apple-to-use-selfies-to-unlock-phones. Accessed 20 Sept 2021

Choi H, Park J, Jung Y (2018) The role of privacy fatigue in online privacy behavior. Comput Hum Behav 81:42–51. https://doi.org/10.1016/j.chb.2017.12.001

Dang LM et al. (2019) A survey on Internet of Things and cloud computing for healthcare. Electronics-Switz 8(7):768. https://doi.org/10.3390/electronics8070768

Dhruva SS, Ross JS, Akar JG (2020) Aggregating multiple real-world data sources using a patient-centered health-data-sharing platform. npj Digit Med 3(1):60. https://doi.org/10.1038/s41746-020-0265-z

Diega GN, Walden I (2016) Contracting for the 'Internet of Things': looking into the nest. Queen Mary School of Law Legal Studies Research Paper 219

Etzioni A (2015) A cyber age privacy Doctrine: more coherent, less subjective, and operational. Brooklyn Law Rev 80(4):Article 2

Feng HX, Li GH, Xu CR (2017) A quality control circle process to improve implementation effect of prevention measures for high-risk patients. Int Wound J 14(6):1094–1099. https://doi.org/10.1111/iwj.12764

Finnegan M, Kapo M (2018) What is windows hello? Microsoft's biometrics security system explained. Comput World. https://www.computerworld.com/article/3244347/what-is-windows-hello-microsofts-biometrics-securitysystem-explained.html. Accessed 20 Oct 2021

Fosch-Villaronga E et al (2018) Cloud services for robotic nurses? Assessing legal and ethical issues in the use of cloud services for healthcare robots. In: 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), University Carlos III of Madrid, Madrid, IEEE, pp. 290–296. https://doi.org/10.1109/IROS.2018.8593591

Gagnon MP, Simonyan D, Ghandour EK, Godin G, Labrecque M, Ouimet M et al. (2016) Factors influencing electronic health record adoption by physicians: a multilevel analysis. Int J Inform Manage 36:258–270. https://doi.org/10.1016/j.ijinfomgt.2015.12.002

Gartner S (2020) 65% of the World's population will have its personal data covered under modern privacy regulations. https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w. Accessed 20 Feb 2022

Gephart SM, Effken JA, McGrath JM (2013) Expert consensus building using e-Delphi for necrotizing enterocolitis risk assessment. Jognn-J Obst Gyn Neo 42(3):332–347

Ghaffary S (2019) Amazon is trying to regulate itself over facial recognition software before congress does. Vox. https://www.vox.com/technology/2019/2/7/18216125/amazon-regulation-facial-recognition-software. Accessed 13 Dec 2022

Greenleaf G, Cottier B(2020) Ends a decade of 62 New Data Privacy Laws Privacy Laws Bus Int Rep 163:24–26. https://ssrn.com/abstract=3572611

Günther M, El Shafey L, Marcel S (2017) 2D face recognition: an experimental and reproducible research survey. No. REP_WORK. Idiap

Haab TC, Whitehead JC, Parsons GR (2010) Effects of information about invasive species on risk perception and seafood demand by gender and race. Resour Energy Econ 32(4):586–599. https://doi.org/10.1016/j.reseneeco.2010.04.008

Hadi H, Brian HN, Fazel A, Burak K, Tolga S (2019) A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustain Cities Soc 50(3):101660. https://doi.org/10.1016/j.scs.2019.101660

Haraty RA, Kaddoura S, Zekri AS (2018) Recovery of business intelligence systems: towards guaranteed continuity of patient centric healthcare systems through a matrix-based recovery approach. Telemat Inform 35:801–814. https://doi.org/10.1016/j.tele.2017.12.010

Hargittai E, Marwick A (2016) What can I really do? Explaining the privacy paradox with online apathy. Int J COMMUN-US 10:3737–3757

Hashem IAT, Chang V, Anuar NB, Adewole K, Yaqoob I, Gani A, Chiroma H (2016) The role of big data in smart city. Int J Inform Manage 36(5):748–758. https://doi.org/10.1016/j.ijinfomgt.2016.05.002

Hill K (2020) The secretive company that might end privacy as we know it. N Y Times. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. Accessed 20 Dec 2021

Hoffmann CP, Lutz C, Ranzini G (2016) Privacy cynicism: a new approach to the privacy paradox. Cyberpsychology 10(4). https://doi.org/10.5817/CP2016-4-7

Horton FW (1985) Information resources management. Nanjing University Publication

Hossain MA, Dwivedi YK (2014) What improves citizens' privacy perceptions toward RFID technology? A cross-country investigation using mixed method approach. Int J Inform Manage 34(6):711–719. https://doi.org/10.1016/j.ijinfomgt.2014.07.002

IBM Security (2022) Cost of a Data Breach Report 2022. https://www.ibm.com/downloads/cas/3R8N1DZJ. Accessed 20 Feb 2023

Iqbal MA, Olaleye OG, Bayoumi MA (2016) A review on Internet of Things (IoT): security and privacy requirements and the solution approaches. Global J Comput Sci Technol 16(7)

Isiaka F, Adamu Z (2022) Custom emoji based emotion recognition system for dynamic business webpages. Int J Intell Comput 15(4):497–509. https://doi.org/10.1108/IJICC-11-2021-0254

Jain AK, Ross A (2004) An introduction to biometric recognition. IEEE Trans Circuits Syst Video Technol 14(1):4–20. https://doi.org/10.1109/TCSVT.2003.818349

Jain AK, Flynn P, Ross AA (2018) Handbook of biometrics. Springer, Berlin

Jain AK, Nandakumar K, Nagar A (2008) Biometric template security. Eurasip J Adv Signal Process 1–17. https://doi.org/10.1155/2008/579416

Ji S, Gui ZY, Zhou TQ, Yan HY, Shen J (2018) An efficient and certificateless conditional privacy-preserving authentication scheme for wireless body area networks big data services. IEEE Access 6:69603–69611. https://doi.org/10.1109/ACCESS.2018.2880898

Kabir S (2017) An overview of fault tree analysis and its application in model based dependability analysis. Expert Syst Appl 77:114–135. https://doi.org/10.1016/j.eswa.2017.01.058

Kachur A, Osin E, Davydov D et al. (2020) Assessing the Big Five personality traits using real-life static facial images. Sci Rep 10:8487. https://doi.org/10.1038/s41598-020-65358-6

Kan M (2015) Alibaba uses facial recognition tech for online payments. Computer World. https://www.computerworld.com/article/2897117/alibaba-uses-facial-recognition-tech-for-online-payments.html. Accessed 20 Feb 2022

Kapoor KK, Tamilmani K, Rana NP, Patil P, Dwivedi YK, Nerur S (2018) Advances in social media research: Past, present and future. Inf. Syst Front 20(3):531–558. https://doi.org/10.1007/s10796-017-9810-y

Karantzoulidis S (2019) This Smart Lock has a built-in facial recognition camera. Secur Sales Integr. http://www.securitysales.com/news/smart-lock-facialrecognition-camera/. Accessed 20 Feb 2022

Kilovaty I (2021) Psychological data breach harms. NCJL & Tech 23:1

Kindt EJ (2013) Privacy and data protection issues of biometric applications: a comparative legal analysis. Springer Netherlands, New York. https://doi.org/10.1007/978-94-007-7522-0

Knight W (2017) In China, You Can Pay for Goods Just by Showing YourFace. MIT Technol Rev. http://technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face/. Accessed 21 Feb 2022

Komendantova N, Ekenberg L, Svahn M, Larsson A, Shah SIH, Myrsini Glinos, Koulolias V, Danielson M (2021) A value-driven approach to addressing misinformation in social media. Humanit Soc Sci Commun 8:33. https://doi.org/10.1057/s41599-020-00702-9

Kshetri N (2014) Big Data's impact on privacy, security and consumer welfare. Telecommun Policy 38:1134–1145. https://doi.org/10.1016/j.telpol.2014.10.002

Kumar S, Singh SK et al. (2018) Privacy preserving security using biometrics in cloud computing. Multimed Tools Appl 77(9):11017–11039

Kwon O, Lee N, Shin B (2014) Data quality management, data usage experience and acquisition intention of big data analytics. Int J Inform Manage 34(3):387–394. https://doi.org/10.1016/j.ijinfomgt.2014.02.002

Li T, Zheng YH, Zhou T (2017) Efficient anonymous authenticated key agreement scheme for wireless body area networks. Secur Commun Netw 8. https://doi.org/10.1155/2017/4167549

Li WD (2020) The connotation, elements and composition of the Internet of Everything. Acad Front 6:40–45

Liang ZQ, Lin DS (2017) Information security risk assessment mechanism research based on power system. Netinfo Secur 4:86–90

Liu YQ (2015) The requirement analysis on exploitation and utilization of personal information in the Big Data Environment. Res Lib Sci 15:67–76. https://doi.org/10.15941/j.cnki.issn1001-0424.2015.15.013

Lyon D (2017) Digital citizenship and surveillance surveillance culture: engagement, exposure, and ethics in digital modernity. Int J Commun-US 11(19):824–842

Mahmoud R et al (2015) Internet of Things (IoT) security: current status, challenges and prospective measures. In: 2015 10th International Conference For Internet Technology and Secured Transactions (ICITST). IEEE, pp. 336–341

Mahoney J, LeHong H (2012) Innovation Insight: the "Internet of Everything" innovation will transform business. Gartner https://www.gartner.com/doc/1886915/innovation-insight-internet-everything-innovation. Accessed 20 Dec 2022

Mainor AC, Patricia AB (2019) Understanding the Internet of Nano Things: overview, trends, and challenge. e-Cienc Inf 9(1):1–30. https://doi.org/10.15517/eci.v1i1.33807

Mao ZJ, Mei H, Xiao YM et al. (2020) Risk assessment of smart city information security based on Bayesian network. J Modern Inf 40(5):19–26

Mayer-Schönberger V, Cukier K (2013) Big data: a revolution that will transform how we live, work and think. Houghton Mifflin Harcourt, Boston

Mehmood R, Selwal A (2020) Fingerprint biometric template security schemes: attacks and countermeasures. In: Singh PK, Kar AK, Singh Y, Kolekar MH, Tanwar S (eds) Proceedings of ICRIC. Springer International Publishing, Cham, pp. 455–467

Millard CJ (2013) Cloud computing law. Oxford University Press, Oxford, p. 2

Miraz MH, Ali M, Excell PS, Picking R (2015) A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT), 2015 International Technology Applications (ITA), pp. 219–224

Moritz B et al. (2021) Making sense of algorithmic profiling: user perceptions on Facebook. Inf Commun Soc 1–17. https://doi.org/10.1080/1369118X.2021.1989011

Nandakumar K, Jain AK (2015) Biometric template protection: bridging the performance gap between theory and practice. IEEE Signal Process Mag 32(5):88–100. https://doi.org/10.1109/MSP.2015.2427849

OECD, OECD Digital Economy Outlook (2020). OECD Publishing, Paris. https://doi.org/10.1787/bb167041-en

Oliver D (2019) Facial recognition scanners are already at some USAirports. Here's what to know. USA Today. https://www.usatoday.com/story/travel/airline-news/2019/08/16/biometric-airport-screening-facial-recognition-everythingyou-need-know/1998749001/. Accessed 17 Jul 2022

Ozgur L, Alkan O (2020) Risk assessment of sea rescue activities on search/rescue ships using L type matrix method. J Home-Page 3(2):66–78

Palattella MR, Dohler M, Grieco A et al. (2016) Internet of things in the 5G era: enablers, architecture, and business models. IEEE J Sel Area Commun 34(3):510–527. https://doi.org/10.1109/JSAC.2016.2525418

Patel P, Bhatt B, Patel B (2017) Human body posture recognition-A survey. In: International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bengaluru, India, IEEE, pp. 473–477. https://doi.org/10.1109/ICIMIA.2017.7975660

Pearson B (2018) 3 Ways retailers can use facial recognition to create computer security. Forbes. http://www.forbes.com/sites/bryanpearson/2018/03/15/3-ways-retailers-can-use-facial-recognition-to-expressbetter-experiences/. Accessed 14 Feb 2023

Perlroth N (2016) Hackers used new weapons to disrupt major websites across U.S. NY Times. http://www.nytimes.com/2016/10/22/business/internetproblems-attack.html?_r¼0. Accessed 14 Feb 2023

Petroff A (2016) MasterCard launching selfie payments. CNN Money. https://money.cnn.com/2016/02/22/technology/mastercard-selfie-pay-fingerprint-payments/index.html. Accessed 17 Jul 2022

Raposo VL (2022) (Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation. Inf Commun Technol 1–19. https://doi.org/10.1080/13600834.2022.2054076

Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40(3):614–634. https://doi.org/10.1147/sj.403.0614

Romero M (2019) Portland gas station using facial recognition technology to curb crime. KGW. http://www.kgw.com/article/news/local/portland-gas-stationusing-facial-recognition-technology-to-curb-crime/283-8ce9f30a-2ac8-4c07-9ea9-11518a75e40a. Accessed 17 Jul 2022

Ruijters E, Stoelinga M (2015) Fault tree analysis: a survey of the state-of-the-art in modeling, analysis and tools. Comput Sci Rev 15(3):29–62. https://doi.org/10.1016/j.cosrev.2015.03.001

Sepas-Moghaddam A, Correia P, Nasrollahi K et al. (2019) A double-deep spatio-angular learning framework for light field based face recognition. IEEE Trans Circuits Syst Video Technol 30(12):4496–4512. https://doi.org/10.1109/TCSVT.2019.2916669

Seubert S, Becker C (2019) The culture industry revisited: sociophilosophical reflections on ‘privacy’ in the Digital Age. Philos Soc Crit 45(08):930–947. https://doi.org/10.1177/0191453719849719

Shiau WL, Dwivedi YK, Yang HS (2017) Co-citation and cluster analyses of extant literature on social networks. Int J Inf Manage 37(5):390–399. https://doi.org/10.1016/j.ijinfomgt.2017.04.007

Smith M, Mann M, Urbas G (2018) Biometrics, crime and security. Routledge, New York

Spyros GT (2018) Ethics and Law in the Internet of Things World. Smart Cities 1:8–120. https://doi.org/10.3390/smartcities10100062018

Sundar SS (2020) Rise of machine agency: a framework for studying the psychology of human–AI interaction (HAII). J Comput-Mediat Commun 25(1):74–88. https://doi.org/10.1093/jcmc/zmz026

Tengyuen N (2017) Webcam face recognition security software and bio-metrics password manager. GECKO FLYURL. https://www.geckoandfly.com/4068/webcam-facerecognition-security-software-and-password-managerprogram/. Accessed 25 Dec 2022

Toor A (2017) This French School is using facial recognition to find out when students aren’t paying attention. The Verge 2017. https://www.theverge.com/2017/5/26/15679806/ai-education-facial-recognition-nestor-france. Accessed 20 Sep 2021

Tuyls PP, Skoric BB, Kevenaar TT (2007) Security with noisy data: on private biometrics, secure key storage and anti-counterfeiting. Springer, Berlin

Voigt P, Von dem Bussche A (2017) The eu general data protection regulation (gdpr): A Practical Guide. Cham: Springer International Publishing, Switzerland

Wallace G (2018) Instead of the boarding pass, bring your smile to the airport. CNN Travel. https://www.cnn.com/travel/article/cbp-facial-recognition/index.html. Accessed 20 Sep 2021

Wang HY, Tang SJ, Ding Y, Wang YJ, Li JH (2020) Survey on biometrics template protection. J Comput Res Dev 05:1003–1021

Wang S, Jiang X, Tang H et al. (2017) A community effort to protect genomic data sharing, collaboration and outsourcing. Npj Genom Med 2(33):1–6. https://doi.org/10.1038/s41525-017-0036-1

West DJ (2019) 5 Ways face recognition can transform customer loyalty. FaceFirst Face Recognition Software. http://www.facefirst.com/blog/ways-face-recognitioncan-transform-customer-loyalty/. Accessed 20 Sept 2021

Wolfe-Robinson M (2019) Manchester City warned against using facial recognition on Fans. The Guardian. https://www.theguardian.com/technology/2019/aug/18/manchester-city-face-calls-to-reconsider-facial-recognition-tech. Accessed 20 Sept 2021

Wollerton M (2019) Elecpro’s smart lock scans faces to let people in CNET. https://www.cnet.com/news/elecpros-smart-lock-scans-faces-to-let-people-in-ces-2019/. Accessed 20 Sept 2021

Xu T, An D, Jia Y, Yue Y (2021) A review: point cloud-based 3D human joints estimation. Sensors (Basel, Switzerland) 21(5):1684. https://doi.org/10.3390/s21051684

Yan BN, Ye ZY, Duan ML (2018) Analysis of the causes of personal information security risks of express users—investigation from user’s angle. J Mod Inform 02:91–95

Yuan CF, Zhang YL, Wang JH, Tong JH (2021) Modeling and evaluation of causal factors in emergency responses to fire accidents involving oil storage system. Sci Rep-UK 11(1):19018. https://doi.org/10.1038/s41598-021-97785-4

Zhang JL, Cui GZ (2002) Safety system engineering. Beijing. Coal Industry Press

Acknowledgements

This research was funded by the National Natural Science Fund of China (Grant Nos. 71974060 and 71734002).

Competing interests

The authors declare no competing interests.

Ethical approval

This article does not contain any studies with human participants performed by any of the authors.

Informed consent

This article does not contain any studies with human participants performed by any of the authors.

Additional information

Correspondence and requests for materials should be addressed to Weidong Li.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.