Chapter 2
Predictive Computing and Information Security: A Technical Review

2.1 Introduction

Future of computing depends upon the effective integration of existing technologies and computing techniques. Integration of cloud computing and IoT provides a new dimension to computing known as 'Predictive Computing' and opens the new possibilities to researchers and developers. Predictive computing utilizes the data to make real-time or near real-time predictions for making life easier and comfortable. The predictive computing consists of various smart objects connected via wireless sensor network for collection of the data which gets stored in clouds for further its processing. The possibilities of predictive computing spans over healthcare, transport, travel, sales, smart home like other many sectors. With the rising demand of sensor-based products and applications for making predictions in many sectors also include the security risks and privacy issues related to data collection and data storage.

Use of predictive computing is getting popular as it is possible to design a smart environment, capable of monitoring air and water pollution, prediction of weather, earthquakes, detecting forest fires, tsunamis and various types of disasters so that early measures could be taken to reduce their devastating effects. Further, to make tourism sector attractive, the travel industries have come out from existing practice of making prediction based on travellers surveys and expert views to real-time collection of information of travellers location and updates about location in terms of photos, nearby spots and many more. Moreover, the big data analysts can capture the information from various photos posted on Facebook and other social networks [1–3]. With the increased use of IoT, a number of smart home appliances have been released into the market that include smart TV, smart refrigerator, smart lights, smart cooling and heating devices that can be controlled by mobile devices or desktops from remote location using internet [4]. Similarly, the use of sensor-based IoT devices is rapidly increasing in predicting the shortest path for vehicle navigation and avoiding of traffic congestion. Vehicle route is predicted in real-time by

P.K. Gupta et al., *Predictive Computing and Information Security*,
DOI 10.1007/978-981-10-5107-4_2

using the existing driving habits in the database and GPS to find the traffic congestion or road block like scenarios [5, 6]. A variety of devices is available in the market to monitor the health of a person. Monitoring of health, using smart blood pressure monitor, glucose monitor, pulse monitoring device, tracking of user activity running, walking, heartbeat, etc., can be done using various sensors and storing of this information over cloud for its further monitoring by healthcare personnel [7]. The healthcare personnel can make the prediction on the basis of received data and can provide suggestion or medications accordingly. In this chapter, we have discussed various such predictive frameworks and computing techniques based on IoT and cloud computing to perform various predictions. As the dependency on these smart devices is increasing and these smart objects are becoming the soft target of attackers to breach the user's privacy. Managing data confidentiality, integrity is becoming a major task it is because a number of restrictions associated with these smart devices in terms limited battery power, lack of complex encryption algorithm, poor access control at user level and lack of secure communication methods, etc. This chapter discusses various information security techniques and frameworks to maintain the confidentiality, integrity, availability and trustworthiness of data. We have listed various available security threats and their countermeasures with respect to two major technologies cloud computing and IoT.

2.2 Google Trend Analysis

With the growing shift towards the use of IoT, cloud computing and predictive computing, we have tried to find and analyze the Google search trends for computing terms like 'Cloud Computing', Internet-of-Things, 'Predictive analytics' and 'Information Security' from year 2008 to 2017 (up to May 2017).

The Google search trend results are shown in Fig. 2.1 and it can be observed that cloud computing and information security are two major areas which lead the global market whereas significant advancements are taking place with IoT and predictive analytics. The authors have also tried to find the trend results for 'Predictive computing' but no results are returned for the same. Market role of predictive computing is gearing up and one can expect a big demand and growth in future with the increased use of IoT 2.0 [8]. We have also analyzed the search trends at region level which are represented in Fig. 2.2 for all the previously mentioned computing techniques. From these results, it is clear that the regions like Singapore, India, Kenya and Uganda are the major regions, related to use of mentioned buzzing words.

Here, Fig. 2.2a represents the top five regions for cloud computing where India lead the search trend, Fig. 2.2b represents the top five regions for information security where Uganda lead the search trend, Fig. 2.2c represents the top five regions for Internet-of-Things and Fig. 2.2d represents the top five regions for predictive analytics, in both the cases Singapore leads the search trends.

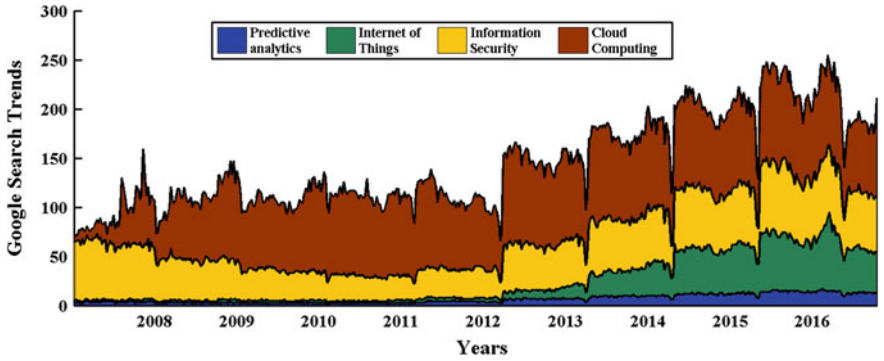

Fig. 2.1 Google search trends for buzzing words cloud computing, information security, Internet-of-Things, and predictive analytics

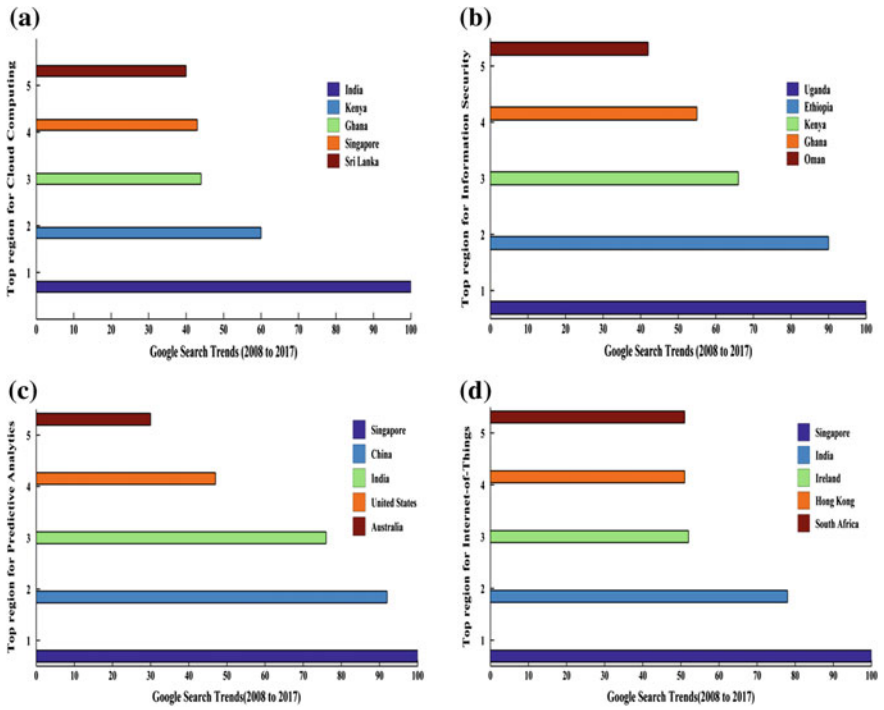

Fig. 2.2 Google search trends versus top 5 regions **a** cloud computing **b** information security **c** Internet-of-Things **d** predictive analytics

2.3 Predictive Computing Techniques

On the basis of performed operations and actions, the predictive computing techniques can be categorized into various categories. In this technical survey, we have tried to incorporate all the recent techniques which are mostly used by the developers to build their predictive solutions.

2.3.1 Data Handling Techniques

With the advancement in technology and computing techniques task of data generation and data processing has become easier. Various technologies like cloud computing, mobile computing, voice recognition, artificial intelligence and advanced application software are making prediction modelling possible. The predictive models are created whenever data is used to train a predictive modelling technique [9]. Table 2.1 summarizes various data handling techniques proposed by various researchers to find patterns in obtained data to perform smart computation.

2.3.2 Sustainable Techniques

Sustainable techniques are used to handle the issue of power consumption of computer systems and its devices. Majority of computer systems and devices are left unattended while they are active where they consume less amount of power. Similarly, if we discuss the same scenario from data centre's point of view then the power by such standalone device becomes disastrous. By using various predictive models and sustainable techniques, we can make predictions about the future of the device and computer system or device can be switched to energy saving state. In [10], Zhu et al. have presented an energy efficient reliable data gathering scheme in wireless sensor network environment. The proposed scheme is based on *Reed–Solomon code* and its enhanced version has been presented with intra-segment and inter-segment coding schemes. The authors have initially defined the optimization problem to derive the proposed energy efficient and reliable packet delivery scheme. In their obtained results, authors have claimed that proposed scheme is applicable in collecting data from sensor nodes at low-rate and low-power. In [11], Khan et al. have proposed a localization scheme *StreetLoc* for energy efficient smart phones using participatory sensing and have focused on the issue of data collection by these participatory nodes from urban streets. Authors have introduced the coverage metrics for the proposed full coverage, partial coverage and k-coverage schemes for the collected data from a street segment of the city. In their obtained results, authors have shown that proposed schemes can save a significant amount of energy. In [12], Abdullah and Yang have considered the issue of energy

Table 2.1 Data handling techniques for predictive analysis

S. No.	Author(s)	Proposed/Applied technique	Technical description	Parameters observed	Limitations and challenges
1	Wang et al. [119]	TVAS	Solved the issue of selection of destination sink node in the sub regions of sensor nodes and switching of aggregation scheme between TVAS and NS	– Time interval – Nearest neighbouring node, and – Data pressure	– Data pressure of sink node depends on threshold value – Metrics used for comparison average hop count, and network life time, and – Complicated concentration model
2	Villari et al. [120]	AllJoyn system	Proposed scalable solution to integrate system with lambda architecture [120] and processing is done using MongoDB	– Uses D-Bus to develop object oriented software independently – Patterns like regular, event based, and automated	– Difficult to handle complex scenarios – No connectivity support for inter domain – Large-scale smart environments management, and – Big data storage
3	Zhu et al. [121]	Permission-based RFID data collection algorithm (PRDC)	Proposed specification language can describe the complex tasks and algorithm is scalable during RFID data collection	– RFID collision – Temporal relations	– Communication overhead – Resource access in large-scale RFID systems
4	Wang et al. [122]	Data collection based on trajectory prediction (DCTP)	– DCTP designed for smart environments – Focused on reduction of incoming data and distributed prediction in real time	– Hidden Markov model – Message (ME) – Prediction of distance (PWD) – Prediction of trigger time (PTT)	– Churning of people is not considered, and – Walking speed is considered as constant

(continued)

Table 2.1 (continued)

S. No.	Author(s)	Proposed/Applied technique	Technical description	Parameters observed	Limitations and challenges
5	Zhu et al. [10]	Enhanced Reed–Solomon (E-RS) code	– Presented inter and intra-segment coding scheme	– Overall energy consumption	– Communication overhead – Lack of security
6	Sharma and Singh [123]	Seed block algorithm (SBA)	– Smart connectivity with remote client in absence of network and remote data backup	– Exclusive OR operation – Seed blocks	– More memory requirement for remote server – Huge difference in processing time
7	Xu et al. [45]	– Semantic data model – Data accessing method (UDA-IoT)	– IoT-based emergency medical services system is designed – Metadata model for ubiquitous data accessing, and – Building real-time system	– Value, annotation, and ontology, and – Entity oriented resource	– Processing cost of data – Coordination of multiple resources, and – Data security issue is not addressed

conservation in IoT and proposed a *message scheduling algorithm* to improve the efficiency of the system. The authors have also handled the faulty and failed node with the proposed algorithm. They have considered two main issues for energy conservation known as saving energy in battery powered objects and quick response to the query and the obtained results show the efficiency and effectiveness in service response and energy consumption. In [13], Brienza et al. have proposed the energy management system E-Net-Manager for various networked computers. They have proposed unique methods to reduce the energy consumption by using the soft sensors of computer systems like keyboard, mouse, bluetooth, Google calendar and PC activity soft sensors. In their results, significant energy saving has been achieved for short idle period. In [14, 15], Gupta and Singh have proposed a novel sustainable algorithm for prediction of CPU workload for minimizing the power consumption by personal computers. They have proposed a prediction model [16, 17] and algorithms for switching the current state of running computer system into power saving state.

2.3.3 Navigation Techniques

One major use of predictive computing is in navigation of vehicles or e-Transportaion. With the growth of technology, it has become possible to predict the shortest route for vehicle navigation. One can predict the navigation paths with lesser traffic rather than considering the busiest road networks in the city. These algorithms usually require a constraint to be placed on the system for effective prediction to take place. A Markov process is a stochastic process in which one can make predictions about the future state of the process based only its current state. Vehicle navigation paths are usually repetitive in nature due to natural constraints that limit the freedom of the driver. One of the most common natural constraints is time where most drivers just attempt to reduce the amount of time spent travelling between their origin and destination. The number of methods has been suggested for the prediction of vehicle navigation paths. Barth and Karbassi [18] have used a hierarchical tree data structure to perform real-time prediction of the navigation path that a vehicle may take for direct trips (source to destination). Their algorithm is recomputed as new data from the vehicle arrives while the vehicle is already in transit. Froehlich and Krumm [19] have discussed an alternative method where details of vehicle navigation path are collected and grouped by similarity. Each specific navigation path is assigned an index and stored. As the vehicle begins journey, the navigation path progresses and the algorithm attempts to match the current navigation path with an existing one. Although this allows for an initial prediction of the navigation path, the prediction is continuously updated as the journey advances. Kansal et al. [20] have discussed a sensor network for tracking using mobile phone devices. They have mentioned the fact that the prevalence of mobile devices and the increased availably of GPS technology makes them ideal nodes in a sensory network that focuses on the same GSM signals used for voice

communication. Trials for autonomous vehicle navigations are on the way and soon one can expect the market release of such cars [21, 22]. Technologies like GPS, RFID [23], sensor networks and IoT have made predictive navigation approaches easier and implementable in all the sectors like automobile, aviation [24] and marine. Cao et al. [25] have used the GPS technology for constructing the minimum dominating set of navigation paths and used this data for selecting the best possible navigation path to drive. The authors have implemented the algorithms like marking process to find the dominating vehicle, Updating process to keep the data updated of neighbour's node, and cutting process to cut down the redundant vehicle information from the database. In [26], Davidson has presented three different algorithms that can be integrated into personal navigation systems. First, algorithm computes positioning for a map aided navigation system designed for land vehicles travelling on road network; second, algorithm is aimed at map aided vehicle navigation indoors and the third algorithm computes solution for the pedestrian navigation system. In [6], Pattanaik et al. have presented a smart congestion avoidance technique by estimating the scope of real-time traffic congestion on urban road networks and predicts an alternate shortest route to the destination. This technique utilizes the k-means clustering approach to estimate the magnitude of congestion and applies Dijkstra's algorithm to predict the shortest route. In [27], Su et al. have designed a shortest path computing algorithm for navigation of large commercial vehicles. They have integrated spatial data with the proposed algorithm. Authors have listed various characteristics of commercial vehicles types like bus, truck, trailer and passenger car, etc. Mitton and Rivano [28] have deployed sensors on bicycles to analyze the various road conditions for medical purpose and have gathered the data in real time from the deployed bicycles. The proposed system is in its preliminary stage and a lot of work is still remaining to obtain the results. In [29], Kranz et al. have discussed the concept of embedded interactions of objects in the day-to-day utilities. They have monitored these interactions using IoT. They have also listed various challenges for embedded IoT like Invisibility dilemma, implicit versus explicit interactions, context dependence, etc. They have presented the vision beyond ubiquitous computing for day-to-day computing using IoT. Similarly, in [30–35], the authors have presented the architecture and smart navigation techniques for vehicles and the presented techniques utilize the IoT and sensor networks for navigation of vehicle. Some of the major predictive navigational techniques are shown in Table 2.2.

2.3.4 Intelligent Agents

The vision of smart environment is possible because of growth in computing techniques and use of predictive models. The smart environments utilize the concept of prediction and communication among the various existing objects. This communication involves various intelligent agents at middleware level for remote access and control of information in smart environment. Chen et al. [23] have

Table 2.2 Predictive navigation techniques and their advantages and challenges

S. No.	Navigation algorithm	Purpose	Advantages	Challenges
1	Dijkstra's [124, 125]	To find shortest path with minimum cost	Can find the shortest routes or the routes with the shortest travel times between the origin and the destination	– Considering large number of nodes, and – Achieving better run time
2	Restricted search algorithm [124, 126]		Unlike search the entire circle as in Dijkstra, restricted search with the small area of the remaining part of rectangle	– Considering large number of nodes
3	*k*-top [127, 128]		Algorithm not only finds the shortest path, but also $k-1$ other paths in non-decreasing order of cost. k is the number of shortest paths to find	– Without considering the loops
4	A* search [124, 129]		Instead of finding the next node with the least cost, the selection of node is based on the cost from the start node plus an estimate of proximity to the destination	– Without improving worst case time complexity
5	Bellman-Ford [130]	To find shortest paths from a single source vertex to all of the other vertices	– Provides more efficiency in terms of nodes covered or path travelled – Edge weights in weighted digraph can be negative number	– Issue of scaling as the network topology changes
	A*-ants [131]	To find the best optimized multi-parameter direction between two desired points using electronic maps	A* algorithm is run before ants algorithm and updates (increases) pheromones of its resulted paths in ants algorithm	
6	CARPA [132]	Multipurpose route recommendation algorithm	It includes data preprocessing, accessibility metrics definition, and multi-objective path finding	– Without considering stairs, high curbs and busy intersections of roads
7	Kalman filter-based algorithm [133–135]	To support the navigational function of a real-time vehicle performance and emissions monitoring	Kalman filter-based algorithm generates pose estimation (position and orientation) information, which enables faster and more robust tracking	– Problems associated with Kalman filters is how to assign suitable statistical properties to both the dynamic and the observational models

proposed code centric RFID system, which is used to store the information based on smart agents and provide the instructions to system whenever action has to be performed. Still proposed system does not meet the goals like knowledge representation and situation-aware code interpretation. In [36], Huang et al. have done body posture analysis by using collaborative accelerometer sensors on different parts of human body like on neck, wrist, waist and thighs. They have tried to predict the odd situation with the help of predictive body posture analysis whether there is any accident like scenario or not. They are unable to determine the condition of the body once the accident has taken place and planning to use gyroscope for more accuracy of results for falling like scenarios. Jeong et al. [37], have designed and implemented large-scale middleware for ubiquitous sensor networks. This ubiquitous sensor network supports intelligent event processing, various types of sensors, real-time sensed data and management of collected metadata. Further, the authors are keen to extend the support for a variety of wireless communication protocols like ZigBee, Bluetooth, Code division multiple access, etc. In [38], Taylor et al. have focused on the distribution of electricity in future and proposed cost effective and intelligent solutions for electricity distribution network and management scenarios. In [39], Gaoan and Zhenmin have proposed an intelligent method for measuring the heart rate using mobile acceleration sensor. They have suggested using their proposed real-time heart-tracking algorithm to develop low-cost heart rate monitor device. In [13], Brienza et al. have focused on the issue of energy consumption by ICT devices and suggested some intelligent soft sensor methods like bluetooth based, Google calendar based, activity soft sensors, etc., to reduce the energy consumption using these devices.

2.3.5 Smart Objects Based Computing

With the growth of mobile networks, researchers and developers are targeting mobile devices as a smart object to perform predictive computing over collected data. These mobile devices are also working as a middleware for transferring data from one sensor node to another. In [40], Kortuem et al. have presented the concept of 'Internet of smart objects' and classified smart objects into three different categories (a) activity aware objects, (b) process aware objects and (c) policy aware objects. These smart objects are equipped with embedded display and buttons on it. They have categorized between these objects on the basis of parameters like awareness, representation, interaction and augmentation. Figure 2.3 represents various smart objects that can be connected with mobile like smart devices in a ubiquitous network. In this section, we have summarized various mobile computing techniques for ubiquitous computing of received data as shown in Table 2.3.

Fig. 2.3 Smart objects in a ubiquitous network [3]

2.4 Predictive Computing Frameworks

In [9], Kalechofsky has presented a simple framework for developing predictive and statistical models for modern business. The author has mentioned that predictive analytics includes various techniques like predictive modelling, machine learning and data modelling to make predictions. The predictive analytics, in turn, uses the predictive modelling framework to perform predictive computing. This computing technique can be used in almost every sector like healthcare, travel, marketing, e-commerce, etc., by using their modelling framework.

2.4.1 Healthcare Frameworks

The predictive computing plays an important role in the prediction of health related issues and sending the early alerts to the patients. These healthcare frameworks use various predictive modelling frameworks for predictions and that's why their accuracy may differ from one framework to another. Predictive modelling is widely in use in clinical research and analysis. In [41], Ng et al. have described a scalable predictive platform known as PARAMO (PARAllel predictive MOdelling) that can

Table 2.3 Smart object based various computing techniques

S. No.	Author(s)	Proposed technique	Application	Advantages	Challenges
1	Ko et al. [136]	Middleware architecture		Solves the issue of interoperability between sensor and middleware and provides intelligent service	Compatibility of smart object with sensors and service providers
2	Solanas et al. [137]	Smart health (s-Health)	Concept of smart health lies in between mobile health and smart cities	Data is collected from patients and also from sensing infrastructure of smart cities	Requires interactions between actors like government, physicians, researchers, and practitioners, etc. Privacy and security is a major challenge
3	Bottazzi et al. [138]	Socially aware and mobile architecture (SAMOA)	Framework allows creating roaming social networks for mobile users anytime anywhere	Middleware solution to address social network management details	Lack of security and performance issues
4	Soliman et al. [139]	Smart home application	Integrated IoT, cloud computing, and Zigbee technology to design the application	Easy to use with improved efficiency of data access	No focus on security and privacy like issues and interoperability with other protocols and smart objects
5	Kortuem et al. [40]	Interaction between smart objects	Categorized smart objects in three categories	Included interaction and social aspects in design of smart objects	– Developed workflow models and ad hoc combination techniques, – Implementation of these techniques is still remaining
6	Mitton and Rivano [28]	City bike network	Deployed sensors on city bikes while cycling to gather data related to road, environment, or medical purpose	– New concept to promote eco smart driving using IoT – Basis model is proposed for city bike network equipped with sensors and base stations to collect the data	– Real-time implementation is complex in nature and involves more base stations as bicycle is not a stationary object and deployed sensors on bike have range limitation – For transferring of data with one base station object can't wait at one place
7	Siebert et al. [140]	LASEC algorithm and novel mechanism A-Ack	Collaborative composition approach has been implemented by the algorithm between service providers and A-Ack mechanism restricts the number or exchange messages for each service	– Composition algorithm is designed in such way to minimize the cost while object is not stationary – Network overhead is reduced by minimizing the number of messages to be exchanged	– Two layer model i.e. communication layer and request layer – Continuous energy consumption by nodes while they are in composition with other nodes – Object must be in the range of nodes

be used by many predictive applications. Brooks et al. [42] have stated that healthcare organizations can implement a predictive model that uses business intelligence (BI) to improve clinical efficiency. They have proposed a framework for developing a domain specific BI model for an expert practitioner in the field. In [7], Gupta et al. have proposed an IoT-based cloud centric health framework to monitor user's activities in sustainable health centres. This framework regularly predicts the user's activities and stores the details of various parameters like heart rate, pulse rate, timing of activity session, etc., in the cloud database and sends alerts to health care professionals of the user wherever emergency like scenario arises.

In [43], Lu et al. have presented the SPOC framework for secure and privacy preserving computing in mobile health care. This framework extends its functionality in the pervasive environment and introduces the user-centric privacy controls. In [44], Zhang et al. have presented three tier system architecture for healthcare system based on ubiquitous sensing. Tier-1 consists of various objects equipped with ubiquitously distributed sensor nodes. Tier-2 consists of ubiquitous technologies like wireless sensor networks, internet, WiMAX, 3G/4G, etc., to transfer the sensed data to doctors or medical practitioners. Whereas, Tier-3 is an information processing centre and consists of nodes like medical practitioners, doctors, data centres, servers for processing of collected data related to patient's health and to provide the necessary action to be taken by the patient. Similarly, Xu et al. [45], have proposed the semantic data model for interpreting the IoT data and also a data access mechanism has been proposed for emergency medical services in ubiquitous environment. Hu et al. [46], have also used the IoT network of physical objects for monitoring and predicting the health condition of elder person living at home. They have proposed an intelligent and secure health monitoring framework for finding the elder's activity and elders can use the mobile device for getting connected with the IoT network. In [47], Zhao et al. have presented the predictive model for finding the effect of multiple sclerosis in patients. They have used logistic regression and machine learning techniques in predicting disease course. In [48], Abreu et al. have studied about the recurrence of breast cancer and presented a predictive model based on combination of machine learning techniques for accurate prediction of recurrence events. In [49], Rana et al. have introduced the concept of changing interventions on different datasets and proposed a predictive framework that models interventions explicitly. In [50], Sakr and Elgammal have discussed some major challenges in healthcare systems which can be resolved using modern technologies like cloud computing, IoT and big data. The aspects of these technologies can be different that vary from communication to data storage. Authors have proposed a framework known as '*SmartHealth*' and described its various applications in the healthcare domain. Ifrim et al. [51], have highlighted the current status of the evolution, trends and research on IoT from e-Health perspective and performed a comprehensive survey.

2.4.2 *Smart Home Frameworks*

The potential technology used for designing the smart home varies from simple sensors to detect the position of door to more sophisticated sensor systems where the sensors are equipped into various objects and humans reside inside the house. Mulvenna et al. [52] have examined the role of context aware computing in smart home environment and monitored the activity of each individual in the house. Authors have developed various frameworks for monitoring the activity. These smart objects equipped with the sensor, collects the data about user's offline activity performed at home and continuously transmit it on the Internet. Apthorpe et al. [53] have mentioned that IoT devices have always-on sensors that capture the data constantly about the user's physical environment. They have developed a prediction strategy from the obtained data for passive network observer and to find about the various possibilities related to the user. In [54], Raj has presented a framework for smart monitoring of home and its security in owners absence. He has designed the context aware protocol for this system. This system is secure, reliable and user friendly and combination of Zigbee, Wi-Fi and body area network like technologies. By making the use of pervasive computing this framework is known as smart home system where user is connected with the various devices in home remotely. In [55], Aquino-Santos et al. have also presented the use of ubiquitous computing in developing smart home applications and interoperability of these applications. They have discussed the challenges like isolation of subsystem by executing several instances using hypervisor for the connected devices, and implementing a micro middleware. In [56], Hong et al. have analyzed the user's habits and behaviour in a living space and discussed the context aware model for smart home systems and the proposed model is shown in Fig. 2.4.

This model connects the various household devices with the user behaviour and process the collected information in an intelligent environment.

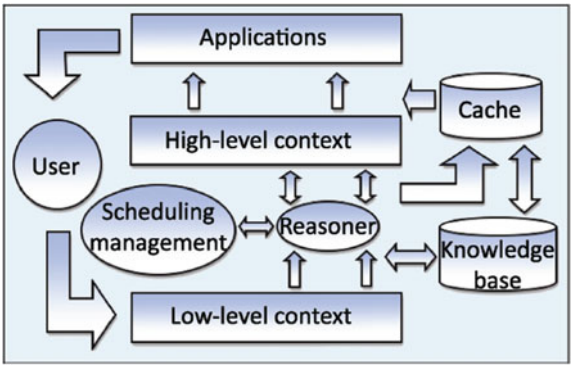

Fig. 2.4 Context aware smart home system model [56]

2.4.3 Navigation Framework

Currently, the road transport of goods or passengers relies on tracking technology. In designing of smart navigation systems, GPS data may be augmented with Wi-Fi and GSM signals to be used to provide location information of vehicle transporting the goods and passengers [57]. At present these systems suffer from limitations like reduced reliability in areas that are not permeated by the necessary GSM or Wi-Fi signals, or areas in which the GPS satellites do not have sufficient coverage. In [5], Malekian et al. have designed and implemented a system which is capable of predicting the navigation path of a vehicle on the basis of the existence of driver's existing driving practices. This system is capable of using RFID based information about navigation paths, in conjunction with predictive algorithms based on the Hidden Markov Model (HMM) to accurately determine the vehicle navigation paths in advance. In HMM, the sequence of observed output values provides information about the sequence of states. If modelled using a HMM, then the observer will only observe a sequence of output tokens directly. Baum et al. [58], have described a model based on this information. The observer can then attempt to infer the sequence of states that yielded the observed output sequence. HMM is an acknowledged tool for predictive solutions to systems that can be modelled as Markov processes. In [59], Simmons et al. have proposed the usage of the HMM to perform predictions on a vehicle's navigation path. In their method, the historical driver data is gathered using GPS information. This is used to supply parameters to the Hidden Markov model. They were able to achieve results of above 98% accuracy in most cases, although the navigation paths they tested had very few places in which choices were required. In [60], Herbert et al. have a proposed a modular framework FaSTrack that provides a safety controller and can be used with most current paths. In [61], Jabbarpour et al. have presented the general framework for vehicle traffic routing system, known as VTRS and used for mitigating traffic congestion on roads. VTRS gathers traffic-related data such as vehicles' speed, travel time and density, user preferences and alternatives paths for preparing the routing tables by calculating the fitness function. In [62], Yang et al. have proposed an autonomic navigation system (ANS) operating over vehicular ad hoc networks (VANETs) for predicting the future vehicle density and adopts hierarchical algorithms for route planning and time dependent routing algorithm for traffic prediction as shown in Fig. 2.5.

In [63], Cebecauer et al. have presented a framework for integrated real-time network travel time prediction of vehicle based on probe data. This framework is capable of predicting short-term traffic conditions, real-time vehicle routing and for trip planning. They have used hybrid probabilistic principal component analysis (PPCA) methodology for short-term prediction of vehicle path. Similarly, a number of frameworks and approaches have been proposed for finding the predictive trajectory guidance, prediction of next turn at road junction and motion planning for autonomous vehicle navigation [64–67].

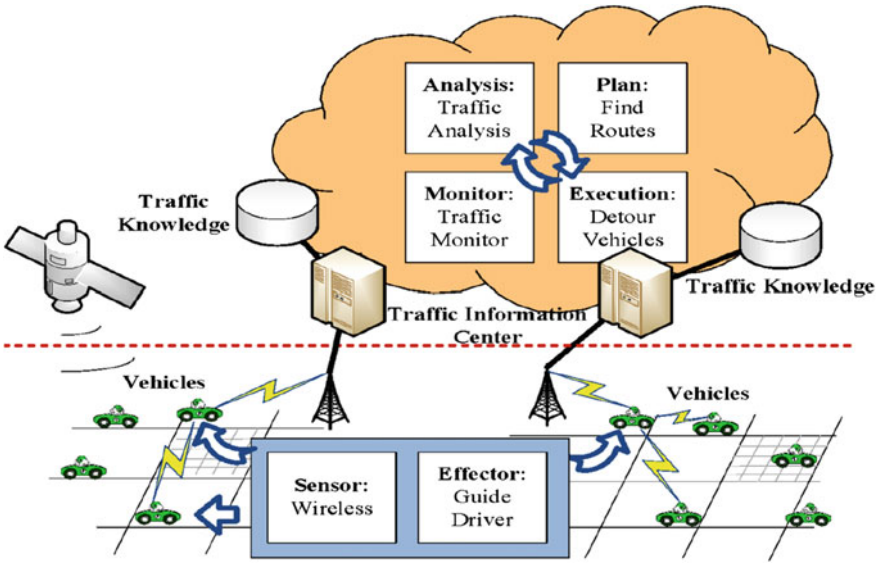

Fig. 2.5 Autonomic navigation system

2.4.4 e-Commerce Framework

Since last decade, a lot of significant developments have taken place in e-commerce market and its applications. The organizations have completely changed the way of marketing by implementing the various data mining rules for predicting the price of product, behaviour of consumer and selecting the appropriate marketing strategy, granting them to make intense and knowledge-driven results. Similarly, change in marketing models is taking place from traditional website based system to knowledge-based system to recommender system. A recommender system predicts about the customer's choice by exploiting ratings made by the customer for the same or similar product in the past. In [68], Qiu has proposed a predictive model, COREL to make purchase behaviour prediction of customers. He has investigated the three factors that significantly affect the purchasing decision of customer in online shopping that is the needs of customers, the popularity of products and the preference of the customers. He has explored associations between products, exploiting them to predict customer needs. In [69], Gupta and Pathak have focused on the dynamic pricing of the product where prices vary according to market demand of the product. Nowadays, dynamic pricing concept is being used by almost all e-commerce sites including retail, automobile, tours and travels, grocery stores and a lot many. They have proposed a model for determining the purchase behaviour and pricing strategy for online customers. This proposed model consists of stages like Data Collection, Preprocessing, Attribute selection, Grouping of customers, Dynamic pricing and Predictive analysis as shown in Fig. 2.6.

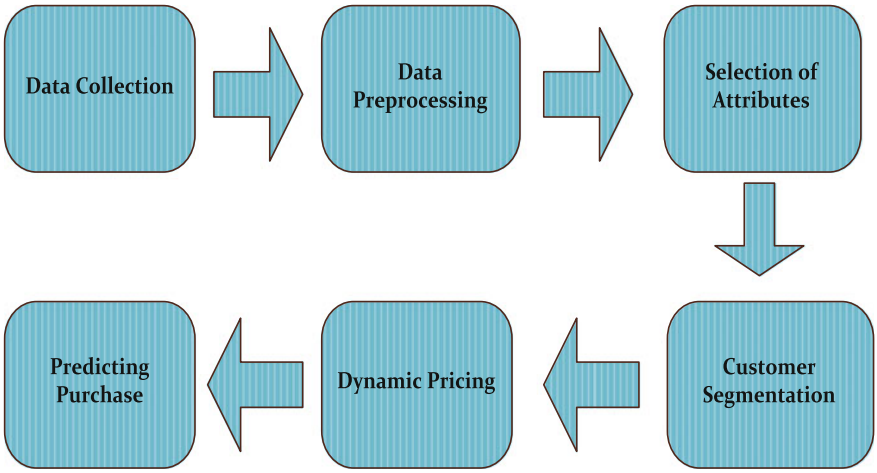

Fig. 2.6 Framework for predicting online purchase based on dynamic pricing

This framework also includes various techniques of Machine learning, Data mining and Statistical methods for predicting the online purchase behaviour of customers by selecting an appropriate price range. In [70], Ahmadi has proposed a framework, e-CLV (Electronic customer lifetime value) for predicting the online customer's behaviour. Proposed model considers real option analysis to predict all future states with probability of each of them. In [71], Lo et al. have tried to characterize, understand the customer's behaviour for developing predictive models of user purchasing intent. They have identified some set of general principles and performed large-scale longitudinal study to model user purchasing intent across many discovery applications. Authors have classified the user's action into four classes known as (i) *searching for a content* (ii) *exploring contents by using provided links* (iii) *getting closer with particular piece of content and* (iv) *saving contents to retrieve it later*. In their predictive analysis, authors have tried to find how engagement in these actions predicts users' future purchasing intent or activity. Similarly, in other studies [72, 73] related to prediction of consumer behaviour, authors have used different perspective of analysis like Badea [72] have used the concept of artificial neural network for predicting consumer behaviour, and Naumzik et al. [73] have performed image sentiment analysis on their proposed model for predicting the increase in rent prices.

2.5 Information Security Techniques

'Data' is becoming a vital component for all kind of computing techniques. Several issues arise with the handling of data like data storage, data access and data usage issues, etc. As discussed earlier, over the period of time various security techniques

have been proposed by the researchers and developers to establish confidentiality, privacy and trust while handling of data. Here we have summarized various security techniques related to cloud computing and IoT.

2.5.1 Security Techniques for Cloud Computing

Security is a major issue in cloud computing as it leads to various types of vulnerabilities while handling of data. Cloud storage and data has to be secured and must ensure various security parameters like authentication, authorization, confidentiality, integrity, availability, etc. In [74], Arockiam and Monikandan have proposed a security technique AROcrypt that ensures confidentiality of data in cloud storage. AROcrypt is one of the symmetric encryption techniques and makes use of ASCII values for processing of plain text into cipher text. In [75], Alsulami et al. have investigated many security techniques and models for cloud computing to main the data integrity and confidentiality. They have identified few of the techniques like encryption, anonymization, separator and multilayering that can have an effect on data integrity and confidentiality. Among these techniques, encryption technique is most widely used for cloud security. In [76], Zhou et al. have presented a scheme to control and prevent unauthorized access to data stored in the cloud. They have proposed a role-based encryption (RBE) technique that integrates the cryptographic technique with role-based access control (RBAC) model. They have also proposed a RBE-based architecture for secure data storage in public cloud. To maintain the privacy of data, policy based encrypted data access approach has been used in which users who satisfy the access policies can decrypt the data using their private key. In [77], another work, Bokefode et al. have used encryption technique AES and RSA for encryption and decryption of data and RBAC used to provide control to users as per their role. In [78], Gugnani et al. have focused on to provide confidentiality to the user while using cloud-based web services, and proposed an approach for selective encryption of XML elements so as to provide confidentiality and to prevent XML document form improper information disclosure. Figure 2.7 represents XML DNA Encryption/Decryption to embed confidentiality. Authors have considered the XPath Injection attacks which take place when web site uses user-supplied inputs to form XPath query for XML data. Terec et al. [79], have discussed the implementation of various cryptographic techniques in Java, MATLAB and Bio-Java and also represented how DNA encryption is implemented in three of them. Besides XML encryption, we have SSL and XML signatures to secure the internet transmission. Users interact with the cloud using XML files and then these XML files and their contents need to be protected so as to safely transfer the confidential information. Also, the communication among Web Service and the clients are mainly done through plain-text XML formats like SOAP messages and WSDL [80].

In [81], Dinesha and Rao have proposed a secure cloud transmission protocol (SecCTP) to maintain data integrity, confidentiality, access management and

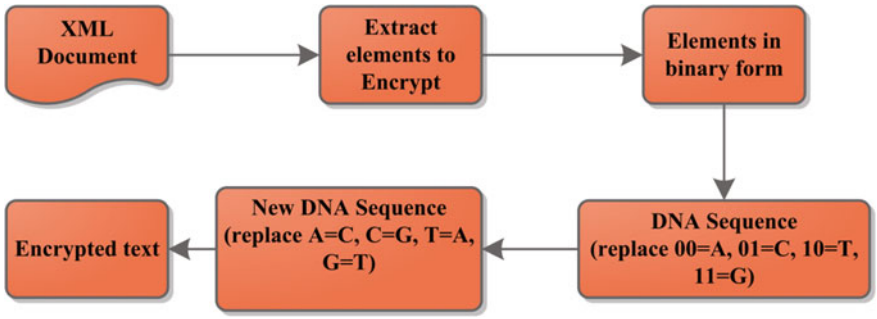

Fig. 2.7 XML DNA encryption approach

identity in the cloud. Proposed technique SecCTP deploys Multi-Dimensional Password (MDP) system, Multilevel Authentication scheme (MLA) and Multilevel cryptography (MLC) system to handle various cloud security issues of authentication, identity and confidentiality. In [82], Yu et al. have proposed an efficient and practical identity based Remote data integrity checking (RDIC) protocol which is based on key-homomorphic cryptographic schemes and maintains perfect data privacy. In perfect data privacy, protocol leaks no information of the stored files to the verifier. In [83], Zhou et al. have stated that the integration of IoT techniques with cloud computing leads to new challenging security and privacy related threats. They have proposed unique security and privacy requirements for cloud-based IoT and addressed the challenging issues of secure packet forwarding and efficient privacy preserving authentication by proposing a new efficient privacy preserving data aggregation without public key-homomorphic encryption. In [84], Choi and Lee have focused on various security issues related to the public sector that restrict any organization from the use of cloud platform. They have proposed a methodology for information security management and adopted a Delphi approach to establish the classification criteria in objective and systematic manner. In [85], Gaetani et al. have focused on data integrity issue in cloud computing and used a *Blockchain-based* method for handling these issues. Blockchain has recently emerged as a fascinating technology that consists of consecutive chained blocks containing records that are replicated on the nodes of a P2P network. These records witness transactions occurred between pseudonyms. They have proposed an innovative blockchain-based database that permits balancing strong integrity guarantees with appropriate performance and stability properties.

2.5.2 Security Techniques for Internet-of-Things

The architecture of IoT converts living and non-living entities into smart objects that can be monitored or used continuously by using internet technologies. These smart objects can communicate with each other, and can respond to the changes in

surroundings intelligently. This intelligent feature derived from IoT architecture includes new security risks and privacy issues. So, maintaining user security and privacy is one of the crucial issues and need to be addressed thoroughly. In [86], Dabbagh and Rayes have presented the security and privacy issues related to IoT platforms. Various security challenges identified by them are Scalability, Multiple verticals, Multiple technologies, Big data, availability, remote locations, etc. They have categorized the IoT architecture into three different domains that include: (a) IoT Sensing Domain, (b) IoT Fog Domain and (c) IoT Cloud Domain. Various security attacks related to cloud domain and IoT are summarized in Table 2.4.

In [87], Nia and Jha have presented a detailed survey and provided a comprehensive list of vulnerabilities and countermeasures against them. Authors have discussed three widely known IoT reference model, i.e. (a) Three-level model [88], (b) Five-level model [89] and (c) Cisco's Seven-level model [90] and discussed various possible applications of IoT. In [91], Singh et al. have discussed state of the art of various lightweight cryptographic primitives that consists of lightweight block ciphers, hash functions, stream ciphers, high-performance systems and low resources devices for IoT environment. They have also analyzed several lightweight cryptographic algorithms like AES, DES, Twine, Seed, RC5, PRESENT, etc., on the basis of their key size, block size, a number of round parameters.

2.6 Information Security-Based Frameworks

As discussed in the previous section, various information security techniques have been evolved to mitigate or to reduce the vulnerabilities in an existing software system, used by business organizations or its customers. For effective implementation of information security and privacy techniques in the system developers and software designers need to modify the existing architecture or framework of software system. It is observed, that in most of the cases these architectures or frameworks are responsible for security-related issues. The reason for this is that security parameters are overlooked by the designers and developers while designing of system. In this section, we have discussed various information security frameworks related to cloud computing and IoT.

2.6.1 Cloud Computing-Based Security Frameworks

Rising demand for storage of data in a cloud environment by the business organizations and customers requires a lot of changes in existing architecture or framework of software systems. Current system design and deployment techniques must be capable enough to accommodate these changes into the system and must ensure the security and privacy of new cloud-based frameworks and architectures. In [92], Chang et al. have presented a multilayered security framework for business

Table 2.4 Security attacks in IoT-based cloud domain

S. No.	Security attacks	Security violation	Reason	Technique(s) to be considered to resolve
1	Hardware Trojans [141–143]	– Confidentiality – Integrity – Availability – Accountability – Auditability – Trustworthiness – Privacy	– Alteration of integrated circuit design – Activation of Trojans based on some external/internal factors	– Circuit design modification, and – Improving Trojan activation method
2	Physical attacks [144–146]		Shared access to components, or network resources	– Hard isolation of devices and software's – Circuit design modification
3	Spoofing/Tag cloning [147]		– Weak security mechanism – Easy to intercept, read and save messages	– Personal firewall – Cryptographic scheme – Hard isolation of devices and software's – Distance estimation – Kill/Sleep command
4	Malicious injection [148]		– Insufficient validation of the input	Pre-testing and validation of inputs
5	Non-standard framework and weak testing [149]		Non-standard coding flaws	– Pre-testing – Designing good framework and policies
6	Virtual machine migration (VM migration) [86]	– Confidentiality – Integrity – Availability	Software bugs, no permission for migration, malfunctioning of device	Server authentication
7	Hidden-channel attack [86]	– Confidentiality	Shared access to components, or network resources	– Hard isolation – Cache Flushing – Noisy data access time, and – Limiting cache switching rate
8	Theft-of-service attack [86]	– Availability	Periodic sampling	– Fine-grain sampling – Random sampling

(continued)

Table 2.4 (continued)

S. No.	Security attacks	Security violation	Reason	Technique(s) to be considered to resolve
9	Insider attack [86]	– Confidentiality – Integrity	Lack of trust	– Homomorphic encryption – Divide the data into multiple chunks and use secret key with certain permutations
10	DoS [150–152]	– Availability – Accountability – Auditability – Privacy	– Node outage because of battery draining – Sending undesired set of requests that seem to be Legitimate – Node outage because of unintended error, sleep deprivation, code injection, etc.	– Securing firmware – Personal firewall, and – Cryptographic scheme
11	Eavesdropping [153]	– Confidentiality – Privacy	– Weak security mechanism – Easy to intercept, read and save of messages	– Personal firewall – Cryptographic scheme – Hard isolation of devices and software's – Blocking
12	Routing attacks [154–156]	– Confidentiality – Integrity – Accountability – Privacy	– Changing routing information	Reliable routing
13	Integrity attacks [157, 158]	– Confidentiality – Integrity	– Manipulating the training dataset – Direct access of server or computing nodes for manipulation	Outlier detection

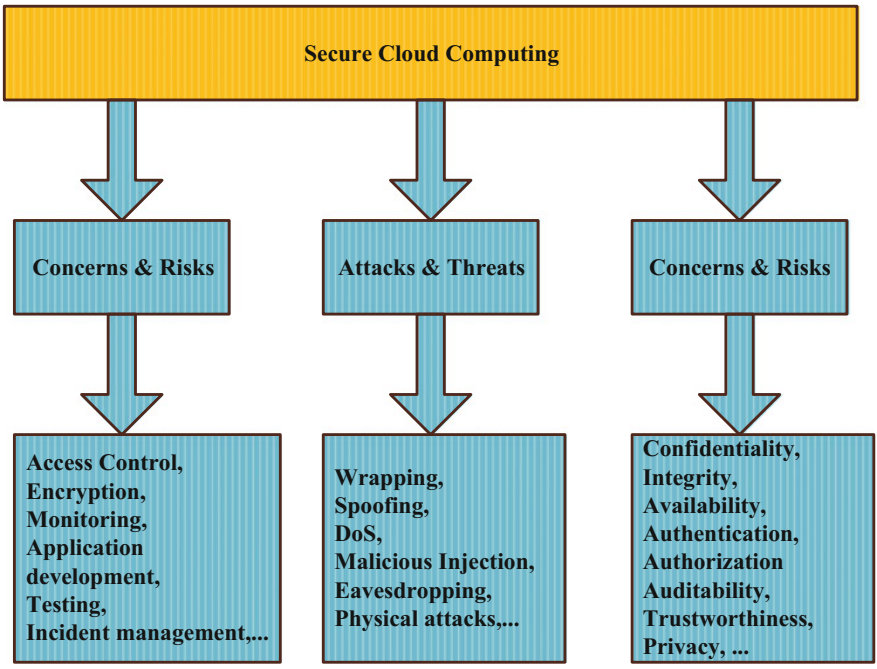

Fig. 2.8 Framework for secure cloud computing

clouds. This Cloud Computing Adoption Framework (CCAF) integrates three major security technologies known as firewall, identity management and encryption. In [93], Mushtaq et al. have presented the quad layered framework for data security, data privacy and data breaches. This layered architecture prevents the confidential information with a variety of quad security layers like Secure Transmission of Data, Encrypted Data and its processing, Database Secure Shell and Internal/external log Auditing. They have also presented a new auditing mechanism where customers can design their own rules for making auditing better. In [94], Youssef and Alageel proposed a framework to identify cloud specific security and privacy challenges, attacks and risks. They have also proposed a security model to perform generic cloud computing and to protect security and privacy requirements from vulnerabilities as given in Fig. 2.8.

In [95], Matte and Kumar have focused on storage of data, and stated that cloud supports data storage in distributed environment. They have provided the solution for security of data in multi-cloud. Multiple copies of data are stored in encrypted form on different clouds. Authors have used plain cipher algorithm for encryption purpose. In another work, Dorairaj and Kaliannan [96] have focused on issue of data migration in cloud, which is accessed by several users. Data protection from unauthorized access becomes important to both organizations and customers. To handle the issue of data sensitivity, authors have proposed an adaptive multilevel

security framework that provides adequate level of security under different classes. This framework provides required access control at each level by using suitable encryption techniques. Similarly, cloud computing-based security framework is being used in every domain like healthcare, vehicle navigation, eLogistics, banking, etc. In [97], Ondiege et al. have mentioned that poor implementation of security in healthcare leaves the patients' data vulnerable to attackers and considered that providing security to remote patient monitoring (RPM) infrastructure is a major issue. They have proposed a new identification technique NFC in their new security framework for monitoring of remote patients in multi-user environment and to keep the patient's information secure. In another work, Jaganathan and Veerappan [98] have proposed a new cloud storage model, CIADS, to keep patient's medical data secure. They have implemented authorization service through certificates, confidentiality by implementing new encrypting algorithm and data integrity is ensured by modified hash algorithm. In [99], Xiao and Xiao have presented the generic ecosystem for cloud security and privacy which employ an attribute driven methodology. This ecosystem employs five security/privacy attributes: (a) Confidentiality, (b) Integrity, (c) Availability, (d) Accountability and (e) Privacy-preservability, as shown in Fig. 2.9. Authors have considered security and privacy separately and demonstrated the connection among vulnerability, threat and defense mechanism for the mentioned attributes in cloud environment.

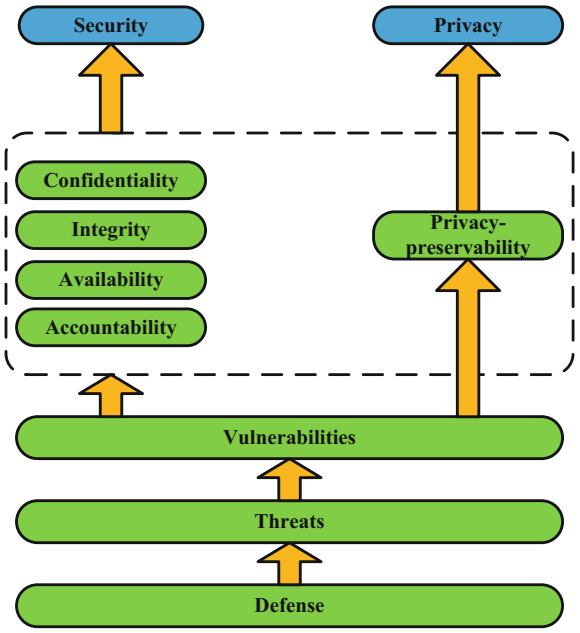

Fig. 2.9 Generic ecosystem based on attributes for cloud security and privacy

2.6.2 IoT-Based Security Frameworks

Significant advancements in the field of information and communication technology (ICT) and wireless technology, lead to development and adoption of various frameworks which are based on cloud computing, IoT, Big data, etc. It is predicted that by 2020, around 50 million of things will be connected to the Internet via IoT [100]. Usage of IoT-based frameworks in every business sector like healthcare, smart home, agriculture, logistics and transportation, is increasing very rapidly as it provides anyone, anytime, anyplace and anywhere type of frameworks for the all connected living and non-living things in the network [101]. However, these technological advancements and adopted frameworks also bring many issues. Security and privacy are considered at the top of all issues that need to handle intelligently for global adoption and use of IoT technology by the humans [102]. Park and Shin [103], have proposed a general security assessment framework for IoT services. They have applied integrated fuzzy multicriteria decision-making (MCDM) approach which uses an analytic network process (ANP) in combination with the decision-making trial and evaluation laboratory (DEMATEL) technique to increase the sensitivity of interrelationships among diverse security requirements. This framework is shown in Fig. 2.10.

In [104], Ge et al. have proposed a framework for modelling and assessing the security of the IoT and provide a formal definition of the proposed framework under five phases known as (a) *data processing*, (b) *security model generation*, (c) *security visualization*, (d) *security analysis and* (e) *model updates*. This framework identifies all possible attack paths in the IoT and evaluates the security level of the IoT through security metrics. In [4], Kang et al. have focused on human centric smart home services and proposed an enhanced security framework for smart

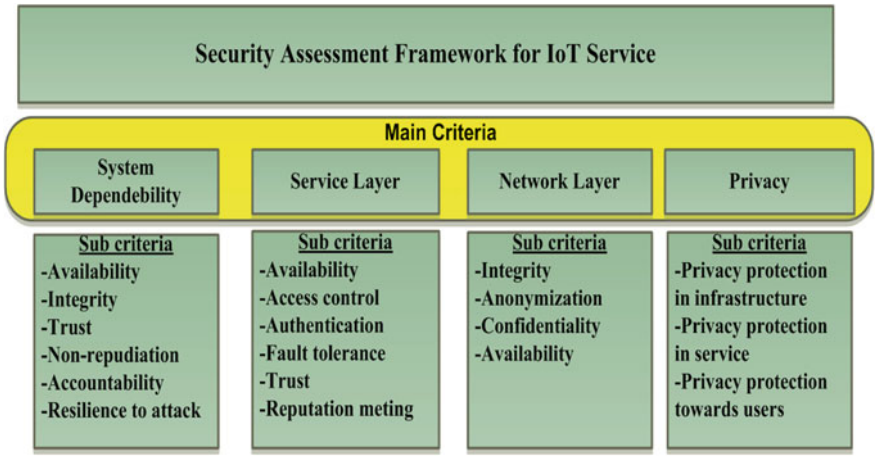

Fig. 2.10 Security assessment framework for IoT

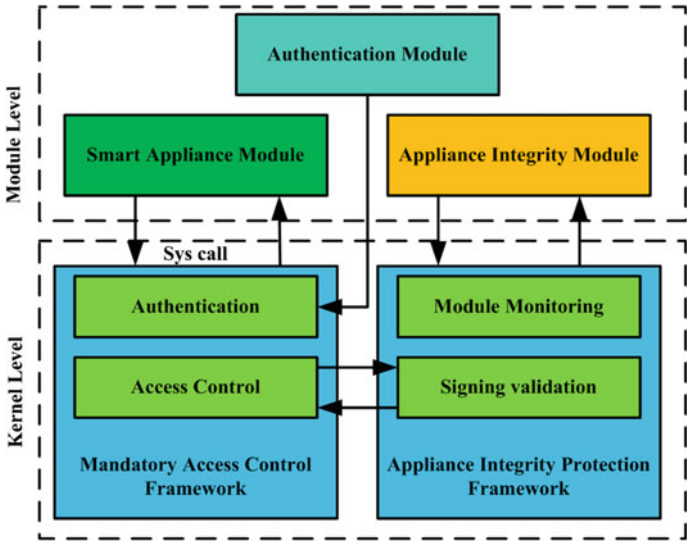

Fig. 2.11 Security framework for smart home

devices in a smart home environment. As shown in Fig. 2.11, this framework is made up of smart appliance module, appliance integrity module, mandatory access control framework and appliance integrity protection framework. This framework provides the security service for ensuring device authentication, integrity and availability.

In [105], Ngu et al. have focused on realization of middleware technologies in IoT systems which represents that software framework play as an intermediary between IoT devices and applications. They have designed an application for real-time prediction of blood alcohol content using smart-watch sensor data and presented a comprehensive survey on the capabilities of the existing IoT middleware. They have also presented a thorough analysis of the challenges and the enabling technologies in developing an IoT middleware. They have captured the key properties of some trusted IoT system as shown in Fig. 2.12. In [106], Ukil et al. have presented privacy preservation framework as a part of the IoT platform and a data masking tool for both privacy and utility preservation. This provides negotiation based architecture to find a solution for utility-privacy tradeoffs in IoT data management. They have also presented a case study on e-Health for this framework.

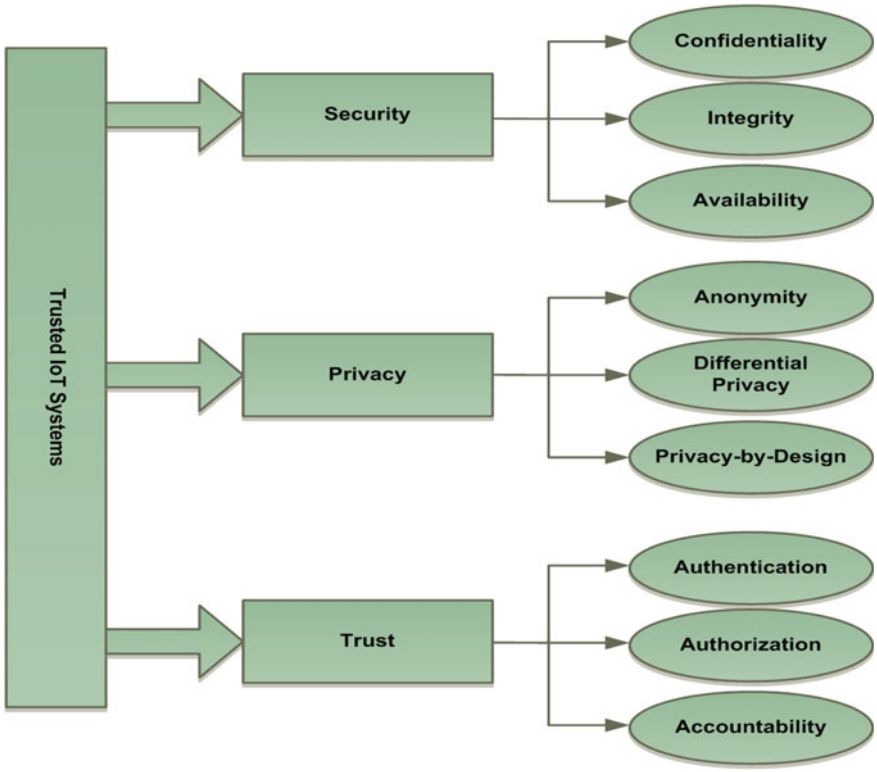

Fig. 2.12 Security, privacy, and trust in IoT systems

2.7 Challenges and Discussions

A primary focus of this chapter is to discuss various techniques and frameworks available for predictive computing and information security. We have found that the security issues in cloud computing and IoT will become a challenging task in near future. According to new research released by TRUSTe, 35% of online US consumers now own at least one smart device other than a smart phone, and the most popular devices are smart TVs (20%), in-car navigation systems (12%), followed by fitness bands (5%) and home alarm systems (4%). In this section, we have summarized few major challenges related to cloud computing and IoT which are listed as follows:

- As per findings from 2015 U.S. IoT Privacy Index, only 79% of consumers are concerned about the idea of their personal data being collected through smart devices, while 69% believed they should own any such data being collected [107].

- In supporting security, privacy and trust mechanisms within IoT middleware has been recognized as a critical and important issue for the successful deployment of IoT applications, and is deemed as one of the major challenges in both industry and academic communities [105].
- As the digital market will be flooded with IoT-based devices and cloud users. It is predicted that by 2020, around 50 million of living and non-living things will be connected to Internet via IoT [100].
- Integration of cloud computing, wireless sensor networks, RFID and other multiple technologies with IoT will increase the complexity of overall system exponentially, as each technology has its own vulnerabilities and integration with IoT will sum up all these vulnerabilities and introduce new security threats to devices and systems [86].
- The modelling security of the IoT is a difficult task as it is characterized by a large number of heterogeneous and mobile devices and facing numerous threats.
- IoT paradigm consists of several verticals that span over e-Health, intelligent transportation, agriculture, smart home, etc. All these verticals have different requirements of security and privacy at device level and at user level.
- IoT framework consists of a number of sensor nodes and scalability of IoT application stored in the cloud, with respect to utilization of CPU, memory and other resources is a challenging task. An IoT solution needs to scale cost-effectively, potentially to hundreds of thousands or even millions of endpoints.
- Another challenge from these endpoints is that they generate heavy amount of data over time and require some effective mechanism in cloud for security and privacy of this data. This large volume of data is also known as Big Data [86].
- The ownership of the data collected from these endpoints must be clearly established and the endpoints and reading devices from the IoT Things should each be equipped with privacy policies. This collected data is further processed to obtain useful information related to health analysis, vehicle route prediction, monitoring a home and environment, etc. [106].
- In [103], Park and Shin have considered service availability challenge at the top priority with increased attention on infrastructure security for networks and systems.
- Further, the nodes in IoT have limited energy and computational power on which implementing complex security measures, is a challenging task. To handle this challenge, security mechanism needs to be developed in context to IoT resources that focus on particular type of attacks like DoS, spoofing, etc., this will help to utilize less energy and computational time.
- In [87], Nia and Jha have also discussed about two emerging security challenges: (1) *Exponential increase in number of weak links*—Currently, available devices in the market don't support complex cryptography algorithms because of these restrictions and this led to number of weak links in the system that can be exploited by the attackers. (2) *Unexpected usage of data*—Growing use of IoT technologies has led to sensor-based connectivity in day-to-day living, this scenario leads to unexpected use of user's data collected by these sensors.

- In another approach, attack paths could be found with the help of framework if node vulnerability and network reachability information is given [103]. The attackers can access these IoT devices and resources with the help of cloud and can use these devices as zombies, so protection of each node becomes important.
- Most of the IoT-based devices are mobile in nature and this mobility has a great influence over security, because attack surfaces changes with the change of network. This challenge involves designing of mobility model for protection of IoT device node in hanging network environment.
- Designing IoT applications and services is yet another challenge as IoT middleware must be available in cloud and on the edges like IoT devices, gateways, etc.
- A big challenge is to ensure the security of IoT application and privacy of users along with semantic service discovery in which a failed IoT service gets replaced with available ones in the network without causing any disruption to the user [105].
- As reported, lack of security mechanisms, auditing mechanisms, data integrity and service level agreements are serious concerns in cloud computing. Some security models have been proposed related to proof of retrievability [108], anonymity based system [109], privacy stabilizing architecture [110], process of access control [111], preserving cloud computing privacy (PccP) model [112] and public auditing mechanism-Oruta [113, 114], to overcome mentioned challenges.
- According to NIST [115], various challenges associated with the cloud computing platform are: designing of policies, standards and procedures that are sufficient to defend organizations from threats.
- The distributing the roles and responsibilities among team members to implement security policy is yet another challenge that should be followed with effective planning at each stage of system's life cycle.
- Implementations of security policies are considered in ad hoc manner in cloud environment to satisfy some set of organizational needs to minimize the risk of threats. The future challenge would involve real-time measures to provide assurance against organizational goals.
- Business outsourcing is common phenomenon of organization and number of organization opt outsourcing to reduce the overall business complexity. The cloud computing facilitates organizations with computational and storage resources at reduced operational cost.
- In cloud environment, data owner lacks full control over outsourced data and finds its management untrustworthy as data may get exposed to various insider and outsider attacks or data leakage related issues could be there [100]. Therefore, maintaining a data confidentiality and privacy is a challenging task to gain users confidence for adopting cloud computing.
- Implementing proper access control mechanism could be challenging issue to maintain user's privacy and unauthorized access to data. As mentioned, in cloud computing data is stored with the third party and in such case implementing a

log monitoring system to analyze the various logs related to a security breach and attacks could be a challenging task [116].
- In clouds, similar to dynamic resource provisioning, automatic resources provisioning is another challenging issue in which by predicting the future demand, resources are allocated and de-allocated from the cloud.
- Server consolidation, and energy efficiency is another big challenge in cloud computing to minimize the power consumption and operational cost of data centers. A key challenge in this is to achieve a good trade-off between energy savings and application performance [117].
- For some specific scenarios, cloud interoperability issue is an emerging challenge where it becomes difficult to integrate existing legacy systems with proprietary cloud APIs to get various cloud services [118].

Integration of cloud computing and IoT provides enormous benefits to the users and organizations in terms of more bandwidth and resources. Due to this reason, it has been widely adopted by the industry but still it has number of issues which need to be addressed and several more challenges are emerging related to applications security and privacy after integration of these technologies.

2.8 Summary

The advancement in computing field has gone through from traditional computing to interactive cloud and IoT-based predictive computing to make our lives easier and comfortable. The predictive computing makes the utilization of wireless sensor network for connectivity of various smart objects with Internet and continuous collection of data from these objects to make predictions related to health, navigation, agriculture, sales, etc. Predictive computing makes effective use of machine learning and data mining approaches to process collected data and produce the results in real time for consideration. However, these technological advancements that predictive computing brings are associated with security risks and privacy issues that need to be addressed thoroughly for effective implementation of predictive systems. Ignoring these risks and issues will adversely affect the system's integrity. In this chapter, we have presented a study on various predictive computing techniques and frameworks that can be applied in a variety of fields including vehicle navigation, sustainable computing, e-health, smart home and e-commerce, etc. As we know, integration of IoT and cloud computing sums up the total possible threats related to user and system in case of predictive computing. We have also presented the various information security techniques and frameworks related to cloud computing and IoT. These security techniques represent various security attacks like hidden attacks, eavesdropping, spoofing, etc., and security violations in terms of confidentiality, integrity, availability, trustworthiness, etc., of data. We have also outlined various challenges related to security and privacy issues of cloud computing and IoT. We hope that in future, researchers and developers

will consider these security and privacy issues and will provide appropriate solutions to these issues at an early stage of system development. Predictive computing is the future that will change the way of application development scenario by changing the existing framework into the predictive framework and will provide short-term or long-term prediction results to enhance the day-to-day life of a user.

References

1. Hendrik H, Perdana DHF (2014) Trip guidance: a linked data based mobile tourists guide. Adv Sci Lett 20(1):75–79
2. Irudeen R, Samaraweera S (2013) Big data solution for Sri Lankan development: a case study from travel and tourism. In: Proceedings of international conference on advances in ICT for emerging regions (ICTer 2). IEEE, Colombo, pp 207–216
3. Dai L (2005) Fast shortest path algorithm for road network and implementation. http://people.scs.carleton.ca/~maheshwa/Honor-Project/Fall05-ShortestPaths.pdf. Accessed 15 Oct 2016
4. Kang WM, Moon SY, Park JH (2017) An enhanced security framework for home appliances in smart home. Hum Centric Comput Inf Sci 7(1):1–12
5. Malekian R, Kavishe AF, Maharaj BTJ, Gupta PK, Singh G, Waschefort H (2016) Smart vehicle navigation system using Hidden Markov model and RFID sensors. Wireless Pers Commun 90(4):1717–1742
6. Pattanaik V, Mayank S, Gupta, PK, Singh SK (2016) Smart real-time traffic congestion estimation and clustering technique for urban vehicular roads. In: Proceedings of IEEE region 10 conference (TENCON), Singapore, IEEE, pp 3420–3423
7. Gupta PK, Maharaj BTJ, Malekian R (2016) A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centers. J Multimed Tools Appl. doi:10.1007/s11042-016-4050-6
8. Columbus L (2016) Roundup of internet of things forecasts and market estimates. https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#17b3fabf292d. Accessed 10 Mar 2017
9. Kalechofsky H (2016) A simple framework for building predictive models. A Little Data Science Business Guide, pp 1–18
10. Zhu YH, Xu J, Li E, Xu L (2014) Energy-efficient reliable data gathering scheme based on enhanced reed-solomon code for wireless sensor networks. In: Proceedings of international conference on smart computing workshops (SMARTCOMP workshops), Hong Kong, IEEE, pp 275–280
11. Khan A, Imon SKA, Das SK (2014) Ensuring energy efficient coverage for participatory sensing in urban streets. In: Proceedings of international conference on smart computing workshops (SMARTCOMP workshops), Hong Kong, IEEE, pp 167–174
12. Abdullah S, Yang K (2014) An energy efficient message scheduling algorithm considering node failure in IoT environment. Wireless Pers Commun 79(3):1815–1835
13. Brienza S, Bindi F, Anastasi G (2014) e-net-manager: a power management system for networked PCs based on soft sensors. In: Proceedings of international conference on smart computing workshops (SMARTCOMP Workshops), Hong Kong, IEEE, pp 104–111
14. Gupta PK, Singh G (2015) A novel human computer interaction aware algorithm to minimize energy consumption. Wireless Pers Commun 81(2):661–683
15. Gupta PK, Singh G (2012) User centric framework of power schemes for minimizing energy consumption by computer systems. In: Proceedings of international conference on radar, communication and computing (ICRCC), India, IEEE, pp 48–53

16. Gupta PK, Singh G (2012) Energy-sustainable framework and performance analysis of power scheme for operating systems: a tool. Int J Intell Syst Appl 5(1):1–15
17. Gupta PK, Singh G (2011) A framework of creating intelligent power profiles in operating systems to minimize power consumption and greenhouse effect caused by computer systems. J Green Eng 1(2):145–163
18. Barth M, Karbassi A (2003) Vehicle route prediction and time of arrival estimation techniques for improved transportation system management. In: Proceedings of intelligent vehicles symposium, IEEE, pp 511–516
19. Froehlich J, Krumm J (2008) Route prediction from trip observations. SAE technical paper 2008-01-0201. doi:10.4271/2008-01-0201
20. Kansal A, Goraczko M, Zhao F (2007) Building a sensor network of mobile phones. In: Proceedings of 6th international conference on information processing in sensor networks (IPSN'07), ACM, pp 547–548
21. Suo H, Wan J, Li D, Zou C (2012) Energy management framework designed for autonomous electric vehicle with sensor networks navigation. In: Proceedings of 12th international conference on computer and information technology (CIT), Chengdu, Sichuan, China, IEEE, pp 914–920
22. Li Q, Chen L, Li M, Shaw SL, Nuchter A (2014) A sensor-fusion drivable-region and lane-detection system for autonomous vehicle navigation in challenging road scenarios. IEEE Trans Veh Technol 63(2):540–555
23. Chen M, Gonzalez S, Zhang Q, Leung VC (2010) Code-centric RFID system based on software agent intelligence. IEEE Intell Syst 25(2):12–19
24. Canino-Rodríguez JM, García-Herrero J, Besada-Portas J, Ravelo-García AG, Travieso-González C, Alonso-Hernández JB (2015) Human computer interactions in next-generation of aircraft smart navigation management systems: task analysis and architecture under an agent-oriented methodological approach. Sensors 15(3):5228–5250
25. Cao H, Wu W, Chen Y (2014) A navigation route based minimum dominating set algorithm in VANETs. In: Proceedings of international conference on smart computing workshops (SMARTCOMP workshops), Hong Kong, IEEE, pp 71–76
26. Davidson P (2013) Algorithms for autonomous personal navigation systems. https://tutcris.tut.fi/portal/files/2307019/davidson.pdf. Accessed 10 Apr 2017
27. Su JM, Chang CH, Yang TP, Chuang CF, Su SY (2014) Development of shortest path computing mechanism with consideration of commercial vehicles characteristics. In: Proceedings of international conference on smart computing workshops (SMARTCOMP workshops), Hong Kong, IEEE, pp 29–34
28. Mitton N, Rivano H (2014) On the use of city bikes to make the city even smarter. In: Proceedings of international conference on smart computing workshops (SMARTCOMP workshops), Hong Kong, IEEE, pp 3–8
29. Kranz M, Holleis P, Schmidt A (2010) Embedded interaction: interacting with the internet of things. IEEE Internet Comput 14(2):46–53
30. Huang W, Su X (2015) Design of a fault detection and isolation system for intelligent vehicle navigation system. Int J Navig Observ 2015(279086):19. doi:10.1155/2015/279086
31. Wang CC, Lien SF, Hsieh YC (2014) Integration of disaster detection and warning system for a smart vehicle. Adv Mech Eng 6:1–7
32. De Silva MWHM, Konara KMSM, Karunarathne IRAI, Lal KKUP, Wijesundara M (2014) An information system for vehicle navigation in congested road networks. SLIIT Res 113–116
33. Kim JH, Kim SC (2013) Design of architectural smart vehicle middleware. Information 16 (4):2443–2455
34. Wang C, Peng G (2015) Application of internet of things in development of e-navigation architecture. In: Proceedings of international symposium on computers and informatics (ISCI 2015). Atlantis Press, Beijing, China, pp 579–586
35. Wan J et al (2014) IoT sensing framework with inter-cloud computing capability in vehicular networking. Electron Commer Res 14(3):389–416

36. Huang YM, Chao HC, Park JH, Lai CF (2010) Adaptive body posture analysis for elderly-falling detection with multisensors. IEEE Intell Syst 25(2):20–30
37. Jeong YS, Song EH, Chae GB, Hong M, Park DS (2010) Large-scale middleware for ubiquitous sensor networks. IEEE Intell Syst 25(2):48–59
38. Taylor GA, Wallom DC, Grenard S, Huete AY, Axon CJ (2011) Recent developments towards novel high performance computing and communications solutions for smart distribution network operation. In: Proceedings of 2nd IEEE PES international conference and exhibition on innovative smart grid technologies (ISGT Europe), Manchester, UK, IEEE, pp 1–8
39. Gaoan G, Zhenmin Z (2014) Heart rate measurement via smart phone acceleration sensor. In: Proceedings of international conference on smart computing workshops (SMARTCOMP workshops), Hong Kong, IEEE, pp 295–300
40. Kortuem G, Kawsar F, Sundramoorthy V, Fitton D (2010) Smart objects as building blocks for the internet of things. IEEE Internet Comput 14(1):44–51
41. Ng K, Ghoting A, Steinhubl SR, Stewart WF, Malin B, Sun J (2014) PARAMO: a PARAllel predictive MOdeling platform for healthcare analytic research using electronic health records. J Biomed Inform 48:160–170
42. Brooks P, El-Gayar O, Sarnikar S (2015) A framework for developing a domain specific business intelligence maturity model: application to healthcare. Int J Inf Manage 35(3): 337–345
43. Lu R, Lin X, Shen X (2013) SPOC: a secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. IEEE Trans Parallel Distrib Syst 24 (3):614–624
44. Zhang Y, Sun L, Song H, Cao X (2014) Ubiquitous WSN for healthcare: recent advances and future prospects. IEEE Internet Things J 1(4):311–318
45. Xu B, Da Xu L, Cai H, Xie C, Hu J, Bu F (2014) Ubiquitous data accessing method in IoT-based information system for emergency medical services. IEEE Trans Ind Inform 10 (2):1578–1586
46. Hu JX, Chen CL, Fan CL, Wang KH (2017) An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing. J Sens 3734764. doi:10.1155/2017/3734764
47. Zhao Y, Healy BC, Rotstein D, Guttmann CR, Bakshi R, Weiner HL, Brodley CE, Chitnis T (2017) Exploration of machine learning techniques in predicting multiple sclerosis disease course. PLoS One 12(4):1–13
48. Abreu PH, Santos MS, Abreu MH, Andrade B, Silva DC (2016) Predicting breast cancer recurrence using machine learning techniques: a systematic review. ACM Comput Surv (CSUR) 49(3):1–40
49. Rana S, Gupta S, Phung D, Venkatesh S (2015) A predictive framework for modeling healthcare data with evolving clinical interventions. Stat Anal Data Mining ASA Data Sci J 8 (3):162–182
50. Sakr S, Elgammal A (2016) Towards a comprehensive data analytics framework for smart healthcare services. Big Data Res 4:44–58
51. Ifrim C, Pintilie AM, Apostol E, Dobre C, Pop F (2017) The art of advanced healthcare applications in big data and IoT systems. Advances in mobile cloud computing and big data in the 5G Era, pp 133–149
52. Mulvenna M, Nugent CD, Gu X, Shapcott M, Wallace J, Martin S (2006) Using context prediction for self-management in ubiquitous computing environments. In: Proceedings of consumer communications and networking conference, Nevada, USA, IEEE, pp 1–5
53. Apthorpe N, Reisman D, Feamster N (2017) A smart home is no castle: privacy vulnerabilities of encrypted IoT traffic. arXiv preprint arXiv:1705.06805, pp 1–6
54. Raj SV (2012) Implementation of pervasive computing based high-secure smart home system. In: Proceedings of international conference on computational intelligence and computing research (ICCIC), Coimbatore, India, IEEE, pp 1–8

55. Aquino-Santos R, Gonzalez-Potes A, Edwards-Block A, Garcia-Ruiz MA (2012) Ubiquitous computing and ambient intelligence for smart homes applications. In: Proceedings of world automation congress (WAC), Puerto Vallarta, Mexico, IEEE, pp 1–6
56. Hong Z, Li P, Jingxiao W (2013) Context-aware scheduling algorithm in smart home system. China Commun 10(11):155–164
57. Ning Y, Zhong-qin W, Malekian R, Ru-chuan W, Abdullah AH (2013) Design of accurate vehicle location system using RFID. Electron Elect Eng 40(8):105–110
58. Baum LE, Petrie T, Soules G, Weiss N (1970) A maximization technique occurring in the statistical analysis of probabilistic functions of Markov chains. Ann Math Stat 41:164–171
59. Simmons R, Browning B, Zhang Y, Sadekar V (2006) Learning to predict driver route and destination intent. In: Proceedings of conference on intelligent transportation systems (ITSX 06), IEEE, pp 127–132
60. Herbert SL, Chen M, Han S, Bansal S, Fisac JF, Tomlin CJ (2017) FaSTrack: a modular framework for fast and guaranteed safe motion planning. arXiv preprint arXiv:1703.07373, pp 1–8
61. Jabbarpour MR, Zarrabi H, Khokhar RH, Shamshirband S, Choo KKR (2017) Applications of computational intelligence in vehicle traffic congestion problem: a survey. Soft Comput 1–22
62. Yang JY, Chou LD, Tseng LM, Chen YM (2017) Autonomic navigation system based on predicted traffic and VANETs. Wireless Pers Commun 92(2):515–546
63. Cebecauer M, Jenelius E, Burghout W (2017) Integrated framework for real-time urban network travel time prediction on sparse probe data. https://people.kth.se/~jenelius/CJB_2017.pdf. Accessed 10 Mar 2017
64. Zhuang Y, Fong S, Yuan M, Sung Y, Cho K, Wong RK (2017) Predicting the next turn at road junction from big traffic data. J Supercomput 1–21. doi:10.1007/s11227-017-2013-y
65. Zhang M (2014) Path planning for autonomous vehicles. http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=5265&context=etd. Accessed 18 Feb 2017
66. Weiskircher T, Wang Q, Ayalew B (2017) Predictive guidance and control framework for (semi-) autonomous vehicles in public traffic. IEEE Trans Control Syst Technol 1–13
67. Lounis A (2015) Toward fully autonomous vehicle navigation using hybrid multi-controller architectures. Graduate theses. http://lounisadouane.online.fr/__Publications/LounisADOUANE_ManuscritHDR.pdf
68. Qiu J (2014) A predictive model for customer purchase behavior in e-commerce context. In: Proceedings of Pacific Asia conference on information systems (PACIS), pp 1–13
69. Gupta R, Pathak C (2014) A machine learning framework for predicting purchase by online customers based on dynamic pricing. Procedia Comput Sci 36:599–605 (Philadelphia, PA)
70. Ahmadi K (2011) Predicting e-customer behavior in B2C relationships for CLV model. Int J Bus Res Manage 2(3):128–138
71. Lo C, Frankowski D, Leskovec J (2016) Understanding behaviors that lead to purchasing: a case study of pinterest. In: Proceedings of 22nd ACM SIGKDD international conference on knowledge discovery and data mining, San Francisco, CA, USA, ACM, pp 531–540
72. Badea LM (2014) Predicting consumer behavior with artificial neural networks. Procedia Econ Finan 15:238–246
73. Naumzik C, Feuerriegel S, Neumann D (2017) Understanding consumer behavior in electronic commerce with image sentiment. In: Proceedings of 13th international conference on Wirtschaftsinformatik, St. Gallen, Switzerland, pp 1264–1266
74. Arockiam DL, Monikandan S (2014) A security service algorithm to ensure the confidentiality of data in cloud storage. Int J Eng Res Technol (IJERT) 3(12):1053–1058
75. Alsulami N, Alharbi E, Monowar MM (2015) A survey on approaches of data confidentiality and integrity models in cloud computing systems. J Emerg Trends Comput Inf Sci 6(3):188–197
76. Zhou L, Varadharajan V, Hitchens M (2013) Achieving secure role-based access control on encrypted data in cloud storage. IEEE Trans Inf Forensics Secur 8(12):1947–1960

77. Bokefode JD, Ubale Swapnaja A, Pingale Subhash V, Karande Kailash J, Apate Sulabha S (2015) Developing secure cloud storage system by applying AES and RSA cryptography algorithms with role based access control model. Int J Comput Appl 118(12):46–52
78. Gugnani G, Ghrera SP, Gupta PK, Malekian R, Maharaj BTJ (2016) Implementing DNA encryption technique in web services to embed confidentiality in cloud. In: Proceedings of second international conference on computer and communication technologies. Springer, Hyderabad, India, pp 407–415
79. Terec R, Vaida MF, Alboaie L, Chiorean L (2011) DNA security using symmetric and asymmetric cryptography. Int J New Comput Archit Appl (IJNCAA) 1(1):34–51
80. Grobauer B, Walloschek T, Stocker E (2011) Understanding cloud computing vulnerabilities. IEEE Secur Priv 9(2):50–57
81. Dinesha HA, Rao DH (2017) Evaluation of secure cloud transmission protocol. Int J Comput Netw Inf Secur 9(3):45–53
82. Yu Y, Au M Ho, Ateniese G, Huang X, Susilo W, Dai Y, Min G (2017) Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Trans Inf Forensics Secur 12(4):767–778
83. Zhou J, Cao Z, Dong X, Vasilakos AV (2017) Security and privacy for cloud-based IoT: challenges. IEEE Commun Mag 55(1):26–33
84. Choi M, Lee C (2015) Information security management as a bridge in cloud systems from private to public organizations. Sustainability 7(9):12032–12051
85. Gaetani E, Aniello L, Baldoni R, Lombardi F, Margheri A, Sassone V (2017) Blockchain-based database to ensure data integrity in cloud computing environments. In: Proceedings of ITASEC, Venice, Italy, pp 146–155
86. Dabbagh M, Rayes A (2017) Internet of things security and privacy. Internet of things from hype to reality. Springer, pp 195–223
87. Nia AM, Jha NK (2017) A comprehensive study of security of internet-of-things. IEEE Trans Emerg Top Comput. doi:10.1109/TETC.2016.2606384
88. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener Comput Syst 29(7):1645–1660
89. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. Comput Netw 54 (15):2787–2805
90. CISCO (2014) The internet of things reference model. http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf. Accessed 11 Apr 2017
91. Singh S, Sharma PK, Moon SY, Park JH (2017) Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Humaniz Comput. doi:10.1007/s12652-017-0494-4
92. Chang V, Kuo YH, Ramachandran M (2016) Cloud computing adoption framework: a security framework for business clouds. Future Gener Comp Syst 57:24–41
93. Mushtaq MO, Shahzad F, Tariq MO, Riaz M, Majeed B (2017) An efficient framework for information security in cloud computing using auditing algorithm shell (AAS). Int J Comput Sci Inf Secur (IJCSIS) 14(11):317–331
94. Youssef AE, Alageel M (2012) A framework for secure cloud computing. IJCSI Int J Comput Sci Issues 9(4):487–500
95. Matte V, Kumar LR (2013) A new framework for cloud computing security using secret sharing algorithm over single to multi-clouds. Int J Comput Trends Technol (IJCTT) 4 (8):2820–2824
96. Dorairaj SD, Kaliannan T (2015) An adaptive multilevel security framework for the data stored in cloud environment. Sci World J 1–11
97. Ondiege B, Clarke M, Mapp G (2017) Exploring a new security framework for remote patient monitoring devices. Computers 6(11):1–12
98. Jaganathan S, Veerappan D (2015) CIADS: a framework for secured storage of patients medical data in cloud. Int J WSEAS Trans Inf Sci Appl 12:22–35
99. Xiao Z, Xiao Y (2013) Security and privacy in cloud computing. IEEE Commun Surv Tutor 15(2):843–859

100. Ning H, Liu H, Yang LT, Cyberentity security in the internet of things. Computer 46(4): 46–53
101. Vermesan O, Friess P, Guillemin P, Gusmeroli S, Sundmaeker H, Bassi A, Jubert IS, Mazura M, Harrison M, Eisenhauer M, Doody P (2011) Internet of things strategic research roadmap. Internet Things-Global Technol Soc Trends 1:9–52
102. Roman R, Zhou J, Lopez J (2013) On the features and challenges of security and privacy in distributed internet of things. Comput Netw 57(10):2266–2279
103. Park KC, Shin DH (2017) Security assessment framework for IoT service. Telecommun Syst 64(1):193–209
104. Ge M, Hong JB, Guttmann W, Kim DS (2017) A framework for automating security analysis of the internet of things. J Netw Comput Appl 83:12–27
105. Ngu AH, Gutierrez M, Metsis V, Nepal S, Sheng QZ (2017) IoT middleware: a survey on issues and enabling technologies. IEEE Internet Things J 4(1):1–20
106. Ukil A, Bandyopadhyay S, Pal A (2015) Privacy for IoT: involuntary privacy enablement for smart energy systems. In: Proceedings of international conference on communications (ICC), IEEE, pp 536–541
107. TrustArc (2015) 35% of Americans now own at least one smart device other than a phone. https://www.trustarc.com/press/35-of-americans-now-own-at-least-one-smart-device-other-than-a-phone/. Accessed 8 Mar 2017
108. Marium S, Nazir Q, Ahmed A, Ahthasham S, Mirza AM (2012) Implementation of EAP with RSA for enhancing the security of cloud computing. Int J Basic Appl Sci 1(3):177–183
109. Wang J, Zhao Y, Jiang S, Le J (2009) Providing privacy preserving in cloud computing. In: Proceedings of international conference on test and measurement (ICTM 2009), vol 2. Hong Kong, China, IEEE, pp 213–216
110. Greveler U, Justus B, Loehr D (2011) A privacy preserving system for cloud computing. In: Proceedings of 11th international conference on computer and information technology, IEEE, pp. 648–653
111. Zhou M, Mu Y, Susilo W, Au MH, Yan J (2011) Privacy-preserved access control for cloud computing. In: Proceedings of 10th international conference on trust, security and privacy in computing and communications (TrustCom), Changsha, China, IEEE, pp 83–90
112. Rahaman SM, Farhatullah M (2012) PccP: a model for preserving cloud computing privacy. In: Proceedings of international conference on data science and engineering (ICDSE), Cochin, Kerala, India, IEEE, pp 166–170
113. Wang C, Chow SS, Wang Q, Ren K, Lou W (2013) Privacy-preserving public auditing for secure cloud storage. IEEE Trans Comput 62(2):362–375
114. Wang B, Li B, Li H (2012) Oruta: privacy-preserving public auditing for shared data in the cloud. In: Proceedings of 5th international conference on cloud computing (CLOUD), Honolulu, HI, USA, IEEE, pp 295–302
115. NIST (2014) Framework for improving critical infrastructure cybersecurity. https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=267567. Accessed 14 Apr 2017
116. Kent K, Souppaya M (2006) Guide to computer security log management. US Department of Commerce, National Institute of Standard and Technology, Gaithersburg, MD, USA, p 16
117. Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl 1(1):7–18
118. Dillon T, Wu C, Chang E (2010) Cloud computing: issues and challenges. In: Proceedings of 24th international conference on advanced information networking and applications (AINA), Perth, Western Australia, IEEE, pp 27–33
119. Wang C, Zhang Y, Song WZ (2014) A new data aggregation technique in multi-sink wireless sensor networks. In: Proceedings of international conference on smart computing workshops (SMARTCOMP workshops), Hong Kong, IEEE, pp 99–104
120. Villari M, Celesti A, Fazio M, Puliafito A (2014) Alljoyn lambda: an architecture for the management of smart environments in IoT. In: Proceedings of international conference on smart computing workshops (SMARTCOMP workshops), Hong Kong, IEEE, pp 9–14

121. Zhu W, Cui X, Hu C, Ma C (2014) Complex data collection in large-scale RFID systems. In: proceedings of international conference on smart computing workshops (SMARTCOMP workshops), Hong Kong, IEEE, pp 25–32
122. Wang C, Peng Y, De D, Song WZ (2014) DCTP: data collecting based on trajectory prediction in smart environment. In: Proceedings of international conference on smart computing workshops (SMARTCOMP workshops), Hong Kong, IEEE, pp 93–98
123. Sharma K, Singh KR (2013) Seed block algorithm: a remote smart data back-up technique for cloud computing. In: Proceedings of international conference on communication systems and network technologies (CSNT), Gwalior, India, IEEE, pp 376–380
124. Flinsenberg ICM (2004) Route planning algorithms for car navigation. http://brainmaster.com/software/pubs/brain/Flinsenberg%20Route%20Planning.pdf. Accessed 17 Apr 2017
125. Parulekar M, Padte V, Shah T, Shroff K, Shetty R (2013) Automatic vehicle navigation using Dijkstra's algorithm. In: Proceedings of international conference on advances in technology and engineering (ICATE), Mumbai, India, IEEE, pp 1–5
126. Fu M, Li J, Deng Z (2004) A practical route planning algorithm for vehicle navigation system. In: Proceedings of fifth world congress on intelligent control and automation (WCICA), vol 6. Hangzhou, China, June, IEEE, pp 5326–5329
127. Eppstein D (1998) Finding the k shortest paths. SIAM J Comput 28(2):652–673
128. Lebedev A, Lee J, Rivera V, Mazzara M (2017) Link prediction using top-k shortest distances. arXiv preprint arXiv:1705.02936, pp 1–5
129. Shahzada A, Askar K (2011) Dynamic vehicle navigation: an A* algorithm based approach using traffic and road information. In: Proceedings of international conference on computer applications and industrial electronics (ICCAIE), Penang, Malaysia, IEEE, pp 514–518
130. Goldberg AV, Radzik T (1993) A heuristic improvement of the Bellman-Ford algorithm. Appl Math Lett 6(3):3–6
131. Salehinejad H, Nezamabadi-pour H, Saryazdi S, Farrahi-Moghaddam F (2008) Combined A*-ants algorithm: a new multi-parameter vehicle navigation scheme. In: Iranian conference on electrical engineering (ICEE 2008), Tehran, Iran, IEEE, pp 154–159
132. Rahaman MS, Mei Y, Hamilton M, Salim FD (2017) CAPRA: a contour-based accessible path routing algorithm. Inf Sci 385:157–173
133. Zhao L, Ochieng WY, Quddus MA, Noland RB (2003) An extended Kalman filter algorithm for integrating GPS and low cost dead reckoning system data for vehicle performance and emissions monitoring. J Navig 56(2):257–275
134. Hu C, Chen W, Chen Y, Liu D (2003) Adaptive Kalman filtering for vehicle navigation. J Glob Pos Syst 2(1):42–47
135. Jin B, Guo J, He D, Guo W (2017) Adaptive Kalman filtering based on optimal autoregressive predictive model. GPS Solut 21(2):307–317
136. Ko E, Kang J, Park J (2012) A middleware for smart object in ubiquitous computing environment. In: Proceedings of 8th international conference on computing technology and information management (ICCM), Seoul, Korea (South), IEEE, pp 400–403
137. Solanas A, Patsakis C, Conti M, Vlachos IS, Ramos V, Falcone F, Postolache O, Pérez-Martínez PA, Di Pietro R, Perrea DN, Martinez-Balleste A (2014) Smart health: a context-aware health paradigm within smart cities. IEEE Commun Mag 52(8):74–81
138. Bottazzi D, Montanari R, Toninelli A (2007) Context-aware middleware for anytime, anywhere social networks. IEEE Intell Syst 22(5):23–32
139. Soliman M, Abiodun T, Hamouda T, Zhou J, Lung CH (2013) Smart home: integrating internet of things with web services and cloud computing. In: Proceedings of 5th international conference on cloud computing technology and science (CloudCom), vol 2. Bristol, UK, IEEE, pp 317–320
140. Siebert J, Cao J, Lai Y, Guo P, Zhu W (2015) LASEC: a localized approach to service composition in pervasive computing environments. IEEE Trans Parallel Distrib Syst 26 (7):1948–1957
141. Salmani H, Tehranipoor MM (2016) Vulnerability analysis of a circuit layout to hardware Trojan insertion. IEEE Trans Inf Forensics Secur 11(6):1214–1225

142. Shila DM, Venugopal V (2014) Design, implementation and security analysis of hardware Trojan threats in FPGA. In: Proceedings of international conference on communications, Sydney, Australia, IEEE, pp 719–724
143. Wehbe T, Mooney VJ, Keezer DC, Parham NB (2015) A novel approach to detect hardware Trojan attacks on primary data inputs. In: Proceedings of WESS'15: workshop on embedded systems security, Amsterdam, Netherlands, ACM, pp 1–10
144. Becher A, Benenson Z, Dornseif M (2006) Tampering with motes: real-world physical attacks on wireless sensor networks. In: Proceedings of international conference on security in pervasive computing. Springer, New York, UK, pp 104–118
145. Anderson R, Kuhn M (1996) Tamper resistance-a cautionary note. In: Proceedings of second Usenix workshop on electronic commerce, vol 2. Oakland, California, pp 1–11
146. Zorzi M, Gluhak A, Lange S, Bassi A (2010) From today's intranet of things to a future internet of things: a wireless-and mobility-related view. IEEE Wirel Commun 17(6):44–51
147. El Beqqal M, Azizi M (2017) Classification of major security attacks against RFID systems. In: Proceedings of international conference on wireless technologies, embedded and intelligent systems (WITS), Fez, Morocco, IEEE, pp 1–6
148. Uwagbole SO, Buchanan WJ, Fan L (2017) Applied machine learning predictive analytics to SQL injection attack detection and prevention. In: Proceedings of 3rd IEEE/IFIP workshop on security for emerging distributed network technologies (DISSECT), Lisbon, Portugal, IEEE, pp 1–4
149. Hong K, Lillethun D, Ramachandran U, Ottenwälder B, Koldehofe B (2013) Mobile fog: a programming model for large-scale applications on the internet of things. In: Proceedings of 2nd SIGCOMM workshop on mobile cloud computing, Hong Kong, China, ACM, pp 15–20
150. Martin T, Hsiao M, Ha D, Krishnaswami J (2004) Denial-of-service attacks on battery-powered mobile computers. In: Proceedings of 2nd conference on pervasive computing and communications (PerCom), Orlando, Florida, IEEE, pp. 309–318
151. Agah A, Das SK (2007) Preventing DoS attacks in wireless sensor networks: a repeated game theory approach. IJ Network Secur 5(2):145–153
152. C´ardenas AA, Amin S, Lin ZS, Huang YL, Huang CY, Sastry S (2011) Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of 6th symposium on information, computer and communications security, ACM, pp 355–366
153. Mukherjee A (2015) Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints. Proc IEEE 103(10):1747–1761
154. Revathi B, Geetha D (2012) A survey of cooperative black and gray hole attack in MANET. Int J Comput Sci Manage Res 1(2):205–208
155. Heer T, Garcia-Morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K (2011) Security challenges in the IP-based internet of things. Wirel Pers Commun 61(3):527–542
156. Wallgren L, Raza S, Voigt T (2013) Routing attacks and countermeasures in the RPL-based internet of things. Int J Distrib Sens Netw 9(8):1–11
157. Barreno M, Nelson B, Sears R, Joseph AD, Tygar JD (2006) Can machine learning be secure. In: Proceedings of symposium on information, computer and communications security, Taipei, Taiwan, ACM, pp 16–25
158. Huang L, Joseph AD, Nelson B, Rubinstein BI, Tygar JD (2011) Adversarial machine learning. In: Proceedings of 4th ACM workshop on security and artificial intelligence, Chicago, IL, USA, ACM, pp 43–58