Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 15 (2020) pp. 001-016
© MIR Labs, www.mirlabs.net/jias/index.html

Security, Privacy Research issues in Various Computing Platforms: A Survey and the Road Ahead

Amit Kumar Tyagi[1], Meghna Manoj Nair[2], Sreenath Niladhuri[3] and Ajith Abraham[4]

[1] School of Computer Science and Engineering,
Vellore Institute of Technology, Chennai Campus, Chennai, 600127, Tamilnadu, India.
amitkrtyagi025@gmail.com

[2] School of Computer Science and Engineering,
Vellore Institute of Technology, Chennai Campus, Chennai, 600127, Tamilnadu, India.
mnairmeghna@gmail.com

[3] Department of Computer Science and Engineering,
Pondicherry Engineering College, -605014, Puducherry, India.
nsreenath@pec.edu

[4] Machine Intelligence Research Labs (MIR Labs),
Scientific Network for Innovation and Research Excellence, Auburn, Washington 98071, USA
ajith.abraham@ieee.org

***Abstract*: Security and Privacy (S&P) preserved systems play an important role in decision support for Internet-mediated service provision. It is essential (need to be mandatory) to enable systems/ users to represent and update their security and maintain privacy with other peers (systems, in open networks) for sharing files, and especially to accessing reliable services in computing/ real world scenarios. Privacy and security concerns are highly critical one and required efficient solution from research communities (working in different domains/ disciplines around the world). The motto of this very article is to provide apprehensive and rightful information about the existing security and privacy issues, approaches, hurdles, etc. in a plethora of platforms to enhance the data quality in the corresponding processing department. Note that among several issues like trust, efficiency, scalability, security, complexity, etc., especially security and privacy issues (in various computing platforms) have been discussed in this work. The review methodology has led to the successful revelations of the major challenges and necessities for safe and secure privacy in real time.**

Keywords*:* Security, Privacy, Trust, Computing Environment, Computer Science.

I. INTRODUCTION

Security is a human right and need to be provided in all situations to client/ user/ system in this smart era (to electronic frameworks). On another side, privacy is required to be maintained for communicated or collected data (data in motion and data at rest). Privacy and Security have different meaning but they are inseparably related. Security can both be an ally and an enemy to privacy. Though privacy and security seem to complement each other, privacy has a socialistic perspective while security has a technical approach. The relationship between them is that the security technologies might provide mechanisms by which privacy can be ensured [1, 3]. Privacy and Security are two integrated issues (important) in the deployment of every technology (require with data, i.e., data need to be secured and confidentially during data transfer) or network.

Security is the degree of confrontation or protective nature from destruction, valuable goods, humans, nation, institution, etc. On the contrary, privacy refers to "masking oneself from others" [1], i.e., securing our personal details, location, etc. from illegal access or rather, privacy refers to the certain information which everyone would like to keep in incognito mode of theirs. For example, in a vehicular ad-hoc network, user's privacy is important while communicating with other users and also with infrastructure, a user always worry about their personal data and their location. Moreover these issues trust issue also comes into picture in computing environment, but this article is more focused towards security and privacy issue only. The difference between privacy and security have discussed (in detail) in [1, 2].

Hence, the organization (remaining part) of this work is followed as: Section 2 discusses about motivation related to this work. Then from section 3 to 14, this work discusses various security and privacy issues in various computing platforms, starting from Big Data to Blockchain technology. And in last, we conclude this work (in brief) with some future enhancements (needed to be done in near future) in section 15.

II. MOTIVATION

It is a mandating fact that human rights, which includes privacy, are to be preserved and secured when users interact and converse with each other on a computing platform. We noticed that, with privacy, trust also an essential component in several computing platforms like Vehicular Ad-hoc Network (VANET), Cloud Computing [5], Grid Computing, Blockchain [29], etc. [11]. Authors in [10] have proven that privacy is indeed a factor that drives trust and loyalty without the direct interaction between privacy and the users' manners (trust). Security is also dependent on Trust component (e.g., in case of insider attack, any security mechanism fails). On the whole, trust leads to a number of definitions as it is completely based on context and the topic in consideration (e.g. ethics and values, computing sciences, socio-economics, etc.) [10]. Trust is based on beliefs, faith and takes years to build. Once it is lost, hard to gain/ recover [10]. It is necessary for users to trust the Recommendation and Reputation (R&R) [12] schemes before R&R can play a role in informing users 'trust perception. It is to be noted that location privacy and trust, both equally demand for interactions, usage of personal info and details, computation and analysis, etc. But, when we make a survey on several computing platforms, then we find that Security, Privacy and Trust are highly critical concerns in the past decade [1]. Security and Privacy are highly essential for every computing platform/ environment, for example, transfer information needed to be secured with good encryption algorithm and needed to be kept confidential along the ways/ network/ channel/ in system. So, we used (explained) these two issues "security and privacy" to discuss in each and every computing platforms. Note that we could not consider trust concerns here (in this work) because trust belongs to belief, faith, etc., and require a lot of time (also interaction) to build. For explaining trust, several metrics, measurement are required to discuss in each computing environment, which will make this article difficult to read (and project). So, authors will try to give trust concerns in various computing environment in separate article (work) in near future. With this survey, we will get to know that there is not a single approach/ trustworthy method which can provide/ overcome these two issues (security and privacy) in the respective computing platforms. In summary, there are several areas where security and privacy issues are rising with a higher growth. And not much research work has been done with respect to some applications/ areas like grid computing, future vehicular network, and Blockchain technology, etc. So, we require a lot of research objectives/ directions/ issues and challenges (also research gaps in current scenarios) to be solved by future researchers with respect to respective computing platforms. Hence, this result provides us a primary motivation to do innovative work in several areas. These emerging factors force us to write this work/ paper. Now this section onwards, we will discuss several security and privacy issues in several computing platforms (as future research directions) in detail. Also, a brief comparison about security, privacy and trust issues is discussed in table 1.

Table 1: Summary of State-of-the-Art and Research Challenges.

S no	Applications / Computing Environment	Objectives	Characteristics	Issues			Research Challenges	Research Opportunities
				Security	Privacy	Trust		
1	Big data	Taking strategic decision, cost optimization	Volume, variety, velocity, variability, value	Vulnerability to fake data generation, presence of untrusted mappers, infrastructure security, reactive security	leakage of sensitive information, Unintentional discrimination, data privacy, data management, conflicting laws in different countries	Data sharing, Data storage, Data processing, quality	Security and privacy in data gathering, storing, analysing, and transferring, lack of efficient tool, timeliness of analysis, scalability	Development of real time processing algorithms ands algorithms for handling domain specific data, Integration of multidimensional data models , creation of Efficient storage devices
2	Cloud computing	Dynamically scalable and virtualised resources are provided as services over internet	On-demand self-service, Broad network access, Resource pooling, Multitenancy of data, Measured service	Data confidentiality, Abuse use of cloud, insecure API, Malicious insider, data leakage, service and traffic hijacking	Data use, share, transfer, archives, unauthorised access	Defining trust according to the attribute of cloud computing environments, handling malicious recommend information, providing different security level of service according to the trust, managing trust degree change w.r.t time and context	Data location, procedure transparency identity and access management, disaster recovery	Increased development of hybrid cloud, Providing more application on cloud, developing a complete security, privacy trust evaluation, management framework
3	Internet of things	Connecting physical devices over a network in secure manner, Online data access and process,	Interconnectivity, heterogeneity, dynamic changes, Things related services	Machine phishing, poor legacy security, IoT malware and ransomware,	Object privacy, Location privacy	Device theft, Data falsification, IP theft, device manipulation	Data storage, Data analytics, Scalability, Inter-operability, network bandwidth constraint, security,	IoT and cloud, IoT and network capacity, IoT and security IoT and smart city, IoT and embedded system

				untrustworthy communication			Privacy, Software development challenges	
4	Internet of everything	The intelligent connection of people, process, data and things, Improve experiences, make smarter decisions, new capabilities	Data input and output, Decentralization and moving to the edge	Spoofing, Tampering, DoS, man in middle attack	Design privacy, Architecture privacy	Self-promotion attacks, Bad-mouthing attacks, Ballot-stuffing attacks, Ballot-stuffing attacks	Security and privacy issues, Network bandwidth	Protecting home users from attack, Enable all security features on all smart devices
5	Fog/ edge computing	Off load cloud node centres, reducing service latency	Heterogeneity, Wireless access, End device mobility, Supports geographic distribution, low latency	Malfunctioning fog nodes, Malicious insider attack, DoS, web security ,wireless security	End user privacy, Location privacy	Authentication, Preserving integrity	Trust, Privacy preservation, Intrusion detection, Access control, cross-border issue and fog forensic	Fog-enabled edge and access networking, Security, Convergence and consistency.
6	Pervasive computing	Combining current network technologies with wireless computing	Decentralisation, Connectivity, Diversification, Simplicity	Cyber foraging, Physical jamming, Eaves dropping,DoS, intrusion	End user privacy, Location privacy, data collection and sharing, Context Dependency	Data sharing, Trusted code, Trusted computing	Scalability, changing environment, private information retrieval	finding ways to integrate existing technologies with a wireless infrastructure, to provide each user with an invisible halo of computing and information services that persists regardless of location
7	Distributed computing	Computing over distributed autonomous computers.	Transparency, openness, Reliability, scalability	Impersonation, DoS, Destruction of data,	Leakage of information	Computational trust	Security, Fault tolerance, Resource sharing	
8	Future internet technologies	Support the complete lifecycle of applications and services that are primarily constructed by recombining existing elements in new and creative ways.	Increased self-manageability, Virtualization of resources, Parallel Internets					Software defined network,
9	Grid computing	enables the integrated, collaborative use of high-end computers, networks, databases, and scientific instruments owned and managed by multiple organizations	Decentralised, Heterogeneity, Resource sharing and coordination, On-demand and high throughput computing.	Architecture issue, Infrastructure issue, Management issue, Grid security, inter-operability, integrity, Authentication	Confidentiality,	Trust relationship, Trust establishments	No clear standard, Limited area and applications, Difficult to develop, Resource sharing between heterogeneous services	managing coordination of multiple resources for distributed applications, formulating effective models for resource-sharing, access negotiation, execution monitoring and control, communication protocols, resource usage accounting and pricing
10	Future vehicular network/ Vehicular Adhoc Network	creation of wireless network for enhancing the data to domain of vehicles	High mobility, Rapidly changing network topology, anonymity of the support, attenuation, frequent exchange of information	Attacks on availability, Attacks on authentication and identification	Data identification, pseudonym	Data centric trust, entity centric trust	Network volatility, Heterogeneity, infrastructure-less, multi hop connection	Secure routing algorithm, development of safety application, Designing integrated system architecture
11	Location	Information		Confidentia	Location	Information	unlink ability	privacy-

	based services	services provided to mobile devices through mobile networks, which may utilize the location information recorded by mobile devices to various value-adding services		lity, integrity, availability	privacy, disclosing user information, Location-based spam, privacy of communication	sharing, untrusted third party	problem, wireless link breakage problem , Collusion of malicious users trouble broad cast storm problem , Operation in multiple responder, Identity privacy ,safety problem, LBS server difficulty, Preserving user location privacy,	preserving LBS, providing reliable, ubiquitous positioning that works anytime and anywhere,
12	Cloudlet	Support interactive and resource-intensive mobile applications, such as those for speech recognition, language processing, machine learning and virtual reality.	Only soft state, powerful, well-connected and safe, builds on standard cloud technology	Virtual Node Security, Mobile Application Security, Virtual Network Security			Proof of cloudlet concept, Balance of offload elements and host mobile device processing, Balance of offload elements via Wi-Fi on cloudlet and mobile operator Internet communicated cloud.	Determine domains where the cloudlet concept with middleware offers better performance for offloading instead of direct communication to clouds, Determine domains where the local mobile device processing is better than using offload elements , Determine balance of local mobile device processing and offload elements
13	Artificial intelligence	Enable computers to perform intellectual tasks as decision making, problem solving, perception, understanding human communication etc.	Eliminate dull tsk, focus diffuse problem, distribute data, Solve dynamic data	National security, data vulnerability, domestic security	Voice and facial recognition, identification and tracking, data exploitation, prediction	AI failure in case of life or death case, cyber security vulnerabilities, Making wrong decision based on AI	Building trust, AI human interface, investment, software malfunction, need of governance	Effect of AI on the supply of and demand for human labor.
14	Block chain technology	Storage of information in secure manner	Decentralisation, Persistency, anonymity, Auditability	Untested code, vendor risk, lack of standard and regulation	Data transparency, auditability , data ownership,	Lack of security, Bit coin, immutable smart contracts	Scalability, privacy leakage, selfish mining	Block chain testing, big data analytics, artificial intelligence, smart contract

III. BIG DATA

The large collection of data/information (generated by a bazillion tech-giant) which is sophisticated to deal with the existing data mining/modern algorithms is what we commonly refer to as Big Data [13]. Here, some challenges with Big Data [14] include analysis, capture, data curation, search, sharing, storage, transfer, visualization, querying, updating and information privacy. Now, issues related to Big Data can be discussed as:

A. *Security issues in Big Data*

It is clear that we are yet to figure out the safe and secure handling of such big data analytics which is extracted from a mightier data environment along with human behaviors. Without a security approach, handling collected data/ information, is too difficult and risky. This collected/ analyzed data contain personal information of users in structured/ unstructured form. Big data is being generated almost in every application like defense, agriculture, medical care, etc. Hence, several studies need to be done in various sectors/ computing platforms. Based on our analysis and observations, security issues and concerns of big data analysis is divided as: input, data processing, output and system wise interactions. Input mainly throws light on all the sensors, hardware devices (along with those involved in IoT network), etc. which are in use. The major concern is to prevent attacks on the sensors. Consider the case of interactions between systems. Security poses to be the largest problem, in summary security and privacy are crucial concerns in current era. Another example would be the hurdles faced when with the data in stock being exposed to duplicate generation of data, existence of unfaithful mappers, problems of alphanumeric protection using cryptography, possibility of data mining and lack of security audits, requirement of highly processing NoSQL databases' evolution, etc. Hence, one major issue with Big Data is generating of large amount of data (rapidly, at a dynamic rate), providing security to data in motion is a critical issue. In general, there are seven security issues available in big data (need attention from research community) include Distributed frameworks, Lack of Designed Security, anonymity concerns, big data skilling gap, Non-relational data stores, Storage, Endpoints, Real-time security/ compliance tool, Data mining solutions and Access controls.

B. Privacy issues in Big Data

In Big Data, privacy is also highly critical issue (i.e., than any other issue, we think). The concern of privacy makes majority of population stay on their heels due to their uncomforted nature because if the systems cannot provide cent percent assurance about safe and sound procurement of personal information, the system fails there. Note that leaking of privacy also raises issue of breaking trust among users and technologies/ organizations. Here, privacy issue has become an essential issue together security in area of big data (because of the value of personal information of users). Big Data analytics makes use of data mining and other apprehension techniques, but the personal details may be leaked to malicious users after the process of analyzing. Consider the example of a shopkeeper. In spite of all the data collected being unidentified (e.g., buying a pistol) as the data is collected from a number of devices, a simple data mining technique can retrieve the details of the person who bought the pistol. Data analysis helps in reduction of the scope of database because the address of the shop and the buyers' age are sufficient enough to pick out the corresponding person. These issues highly recommend the presence of privacy safeguarding. The anonymous (k-anonymity [15], l-diversity [16], etc.), temporary identification, and encryption are some methods in preserving privacy of data analytics, but here some critical factors are like "how to use", "what to use", and "why to use the collected data on big data analytics"?

Hence, this section discusses several critical issues like security, privacy, etc., towards (in) Big Data. Now, next section will deal with several security and privacy concerns, identified in Cloud Computing Environment (CCE) [17].

IV. CLOUD COMPUTING

A computational analysis on a particular internet platform (IBC) that allows shared PC (Personal Computers) to deal with details and resources to PCs and various other systems and devices is called Cloud Computing. It is similar to a pay and use model wherein services are supplied only if requested (e.g., PC systems, servers, stockpiling, applications and administrations). They need a number of centralized administrations to work efficiently in an institution or organization. They have a number of varieties like External Cloud, Internal Cloud, Combined Cloud, etc. Top notch companies are providing clouds services include Amazon EC2 (Elastic Compute Cloud), GoogleApps, IBM's Blue Cloud, Yahoo, Microsoft, Zoho, Mosso, Salesforce, GoGrid and ElasticHosts, etc.

A. Security Issues in Cloud Computing

Safety and security in cloud is procured in bits and pieces with the help of third-party controls similar to those in traditional arrangements. It is to be noted that there are still no common grounds available for cloud computing safety and related issues. At present, a number of cloud providers have executed a plethora of standards for stricter security and they have their own pros and cons. In a standard cloud model, customer organizations are compulsorily adopted to ensure secure services, collection of risk analyses, intense research, and assured activities.

Table 2: Some issues in Cloud Computing Models

IaaS model security issues	PaaS model security issues	SaaS model security issues
1.Virtual Machine (VM) Security 2.Virtual Machines images repository security 3.Virtual network security	1.Structured Query Language related security 2.Application Programming Interface Security	1.Data Security Management 2.Web Application Vulnerability and Scanning

Mostly, the following issues are verified in a general cloud:

- The fear against information resources prevailing in Cloud Computing Environments (CCE).
- The variety of attackers and their capacity of attacking clouds.
- The security risks associated with the cloud, and countermeasures of mitigated threats/ attacks.

Here, some issues have been discussed (based on cloud layers) in table 2. On the whole, safety concerns in Cloud Computing [8, 17] are classified as Traditional concerns, Availability and accessibility issues and Third-Party data control issues.

B. Privacy Issues in Cloud Computing

Data privacy is of utmost importance in cloud services, as cloud providers are able to transfer data from one node to the next which are operated by a number of organizations (from the view of data owner). Once again, trust issues are raised here *hand-in-hand* with privacy. If there's an unauthenticated usage of Personally Identifiable Information (PII), ambiguity and agreement to data flourishing (along with global, dynamic flows, and adhering to the task of acquainting with trans-border data) are taken care of. Issues related to personal safety in cloud, immediately relate to a highly prioritized context as it varies from person to person. Public cloud is best suited for reduction of cost though it relies on Cloud Service Provider (CSP) which is capable of handling ones' data [18]. Hence, this environment uses privacy control, regulatory sophistication, legalized ambiguity, etc. We can conclude that this section discusses a number of important issues in Cloud Computing platform. Now, next section will deal with several security and privacy concerns, identified in Internet of Things (IoTs).

V. Internet of Things (IoT)

The interconnection between various systems and gadgets in different sectors, networks, etc., for efficient usage in vehicles, buildings, and other areas hand in hand with sensors, motors, actuators, etc., is called the Internet of Things (IoT) or Internet Connected Things (ICT) or Smart things [19]. The well-known, Kevin Ashton founded the term in 1999. Note that these devices (embedded with internet of things) collect and exchange a lot data (called Big Data) every day. IoT is not a new concept, it is being used (smart devices are communicating with each other) in various applications (are still in growing phase), i.e., these smart devices have seen a big change in usage since previous decade to till today (roughly 50 billion devices will be connected together till 2030). For applications, IoT devices are using in many applications [20] like smart home, smart grid, smart transportation, smart farming, smart logistics/ supply chain management, Smart e-healthcare, etc.

A. Security issues in Internet of Things (IoT)

Security in Internet of Things is completely new concerns, because IoT are still in accepting phases (yet to embedded in many applications). These devices are making human life easier to live with providing efficient services. On a broader outlook, Internet of Things consists of a rapidly growing network consisting of devices or systems referred to as things [21]. These entities possess their own authentication address and the capability to process and transmit data. When these devices use in a small scale, then leaking of communication/ information may be not an issue, but in case of large-scale applications like Machine-To-Machine (M2M), Device to Device (D2D) communication, etc., security and privacy issues [22] raised in general. There's a pressing need for the presence of secured privacy and trust when it comes to IoT which is done by computing machines and embedded systems like Machine-To-Machine communication (M2M), multifaceted energy grid, home and building automations, interaction between vehicles, etc. Security of such systems needs attention (of researchers) from all over the world. Some issues related to IoT are:

- Access Control: This basically handles the denial and permission of access powers vested to the things in an IoT. It broadly consists of [21]: a) data carriers (Clients) who are responsible for sending or receiving data through the smart devices b) data accessors (things), which communicates with the clients alone. Some challenges with respect to access control (in IoT context) are: "How to handle huge amount of transmitted data (i.e., in the form of stream data) in a common recognized representation"? "How to support the identification of entities"?
- Privacy: Managing privacy or preventing any attack on user's personal information is still in developed phases. Moreover this, several mechanisms like k-anonymity [15], l-diversity [16], t-closeness [23], p-sensitivity [24], etc., have been proposed in the past decade, but not much work have been proposed related to privacy preservation in IoT context. Hence, there is essential requirement for creating efficient privacy preserving mechanisms in IoT context/ devices.
- Policy Enforcement: It concentrates on the perspectives used to implement some efforts in a given system. Policies are basic rules which are made use of in security, consistency of data, etc. However, it is important to identify the enforcement methodology with respect to IoT context (showing a balance between the declaration of privacy and security among the device). We require strong and efficient privacy policies in IoT context to avoid any kind of breaches.
- Mobile Security: Generally, mobile nodes are often commuted from one group to that of another in an IoT network. A number of cryptographic protocol/encryption based mechanisms are made use of for identification, authorisation, and privacy and security in IoT framework. A few rules have been issued in the past years like hash protocol which can easily handle and control the number of overhead communications with tightened security and protection. Security issues relating to mobile phones are under further research for improving the existing methods and mechanisms.
- Secure Middleware: Numerous middleware layers are involved when different technological aspects are put into use for IoT benchmark for integrity, security and data control [22]. Thus, it is necessary to protect the data with its policies along with some secure mechanism. However, this requires the presence of different communication mediums. Many smart devices/ gadgets can support IPv6 communications though they may not acknowledge the IP rules in that local area. Middle wares lack the presence of supervision, and adopt to the IoT conditions. Multidisciplinary approach along with interoperability is a rising concern in this context.
- Authentication and Confidentiality: In the past decade, many attempts have been made by several researchers for authentication and confidentiality (in IoT) like two-way authentication security scheme for IoT, using of Public Key Infrastructure (PKI), etc. All the present solutions and researches solve the issue of lightweight cyphering in chaotic environments but for sophisticated or large-scale networks, these fail drastically. So, it is the need of the hour to create protocols for authorisation and confidentiality in IoT devices.

B. Privacy issues in Internet of Things (IoT)

Privacy is a major challenge in IoT's these days and they need to be protected. IoT devices or entities get unique identifiers/addresses with the help of which it can be easily located throughout the large network. As the devices continuously transmit data in an IoT environment, they also communicate with other devices. Data from different nodes are gathered and analyzed and is used for producing delicate details which may have privacy concerns [20, 21, 22, and 26]. In general, Privacy issues (in the IoTs) are threefold:

- Creating awareness of the privacy risks which are imposed by IoTs which surround data and its subjects,
- Personal control and access over the dispensation of details by encompassing the IoT entities,
- Limiting the subsequent usage and spreading of personal details to the outsiders.

Furthermore, a few other privacy threats and hurdles in the field of IoT are: Identification, Localization, Violation of policies, system attacks, etc. Hence, this section discusses several critical issues like security, privacy, etc., in IoT. Now, next section will deal with several security and privacy concerns, identified in Internet of Everything (IoE).

VI. INTERNET OF EVERYTHING (IOE)

Indeed, with every leap comes a downfall and this is applicable in this context too. The IoT is a world filled with exciting and innovative technical inventions but there are a few hurdles which are yet to be overcome. Cisco laid foundation for the emergence of the Internet of Everything in 2012 and describes it to be the “intelligent interconnect between data, people, processes, and entities” [27]. All forms of communications and interactions were considered to be synonymous between machines, for example, M2M techniques, etc. However, IoE involves all devices in its environment, i.e., which have the interconnection between other smart devices/ gadgets (in all possible applications) [27, 28]. IoE involves Machine-To-People (M2P) and People-To-People (P2P) interactions. More than 2.5 quintillion bytes of information are generated every day (by smart devices) [28]. By 2020, there will be more than 40 trillion gigabytes (or 40 yottabytes) of computerized information or 5,200 GigaBytes (GB) for each individual (on earth) [14]. Note that each smart device/ machine contains quick development process, information generation and transmission, and can be identified each device based on IP address (IPv4/ IPv6). Internet Protocol (IP) is helping in connected unconnected objects, people, things, and processes to networks (i.e., which are connecting for the first time). The Internet Protocol version 6 (IPv6) allows to connect trillions of trillions of devices with the Internet. Note that Internet Protocol (IP) is a basic protocol used for data communication.

A. *Security issues in Internet of Everything (IoE)*

IoT is a subdivision of IoE in broad terms and visualization aspects [28]. It consists of physical or virtual objects and entities which can be made accessible and can be permitted to transmit data without human-machine interactions. But with People-To-People (P2P) or Machine to People (M2P) interactions, IoE faces several security risks like cyber-security challenges, etc. Human experts build and maintain "tougher digital locks" (using Blockchain concept [29]) and "higher firewalls" against cyber-attacks and not enough strong to face IoE's potential attack [7, 28]. However, extensive research in this field can result in projecting the flaws related to TCP/IP and the hurdles of an IT system or network.

B. *Privacy issues in Internet of Everything (IoE)*

Privacy and security issues emerge with increase in the quantity and volume of data being handles, particularly by or related to individuals. Lawmakers must realize the need for striking a balance between protections and granting access in service provisions and product development. Emerging ideas, techniques and mechanisms, like location-based services, are pushing privacy concerns into limelight, offering the users an enhanced experience while portraying concerns of identity protection. Some other issue/challenges are:

- Network infrastructure improvements.
- Building intelligence into the network.
- Distributing computing and storage.

Hence, this section discusses several critical issues like security, privacy, etc., in Internet of Everything. Now, next section will discuss respective issues in fog computing environment.

VII. FOG COMPUTING

Todays’ the mode of computing has moved from distributed, parallel, grid, cloud to Fog/ Edge computing, because large amount of data is being generated by Internet of Things (IoT)/ smart devices/ IoT Based Cloud [30]. This large amount of information (generated by IoT/ internet connected devices) become a critical issue (for data processing and analytical prediction using cloud computation/ existing mining/ machine or deep learning algorithms). Cloud computing is used as backbone to Internet of Things, and provide resource utilizations (accessing) from anywhere, anytime. But, still cloud computing has some limitations. Today’s many problems have been investigated with cloud computing which are: high latency (i.e., time interval between the stimulation and response), limited bandwidth, low internet connectivity, no data center etc. The solutions to such issues can be raised by the introduction of fog computing with an efficient functioning of cloud network, i.e., based on arrangement of nodes referred to as micro clouds which are very close to data sources.

Fog computing or networking or fogging facilitates computation away from a centralized administrative platform to the logical stream of the network [30, 31]. Fog literally means someone closer. Thus, fog computing can be defined to be close to cloud and nearer to the clients. It expands the traditional practices to the nook and corner of the network. It is capable of ranging the foundational blocks of cloud like storage necessities, network services, computation, etc. to the fog nodes, entities, etc. Fog nodes showcase a number of distributed points for data arrangement which are produced by the entities through substitutes, routers, etc. It has the following features [30]: less dormancy and positional awareness, complements geographic distribution, entity mobilization, wireless access, non-uniformity, etc.

A. *Security issues in Fog computing*

Fog computing used in serval applications like smart grid, smart cities, smart logistics, smart vehicles, etc. Several serious issues with respect to fog computing have been investigated from 2012 (this term was coined this year) to till date. The key aspects of safety techniques are authorization, tightening of network security, Intrusion Detection System (IDS), maintaining privacy and building trust, recovery, etc. For example, security of data, security for smart grid, securing virtualization of a critical and essential task, privacy and trust in a sensitive communication [30], etc., are some serious concerns to take care in fog computing environment.

B. Privacy issues in Fog Computing

Confidentiality or Privacy during Network fortification/ access control to a network is a serious concern. Leaking or accessing to user's personal information by malicious user may create several problems. Note that trust is directly connected to privacy concerns, for example, inside attacker or insider (in an environment/ organization) may steal the information of users and can use this information for its financial purpose. Similar network privacy is a serious concern in fog computing. Network operators are capable of producing configurations physically and manually while fog nodes involve a mighty maintenance cost. High risks of data leakages are gaining great attentions while working with networks. The clients gain insight into further information through fog nodes, i.e., larger quantities of details can be gathered by fog nodes when compared to a remote cloud network.

In summary, fog computing for Big Data/ IoT data analytics is in evolving phase and requires innovative research (or efficient solutions) to produce more knowledge and smart decisions. Some other issues [30] in fog computing are: network management, delay in computing, placement of fog servers, energy consumption. Hence, this section discusses several critical issues like security, privacy, etc., in Fog Computing. Now, next section will discuss respective issues in pervasive computing environment.

VIII. PERVASIVE COMPUTING

Hidden computational devices are used for retrieving personal data in order to derive user context leading to a spread of fear amongst the clients about their privacy. On the contrary, smart devices exchange and portray the personal information among other smart systems in a persistent environment. When devices belong to a number of different domains, privacy becomes an issue then. It is indeed a herculean task to develop and produce services which are highly sensitive to privacy in a pervasive environment to optimize the true perks of these techniques and decrease the possible risks. These techniques gather huge amounts of personal details including email-id's, location, etc. But in the current era, with people being highly concerned about their very own details being leaked, majority of them are reluctant to actively take part in a persistent environment. This calls for the generation of a mechanism that assures centum privacy to all its clients. Pervasive computing also known as Context awareness computing or Ubiquitous Computing, has its features described by the authors of [32]:

- Better expansion of smart environments and objects, and impetus behind data collection;
- Data collection will be made more hidden and abstract;
- Gathered data will involve the intimate feelings of individuals;
- Forcing the flow of unnecessary details at a lower level.

It is to be observed that clients using pervasive computing environments are not aware of what is being processed with their personal information and are under the assumption that a service may store or process the data in other ways which may not be authorized by them. This makes clients insecure about their private life and even today, privacy and security are a major concern in majority of the fields. Hence, some serious issues like security and privacy in this environment discussed as:

A. Security issues in Pervasive Computing

Having the maximum communication is being made through wireless technologies; security is a main concern in pervasive computing (when many peer nodes arbitrarily join and leave a network). Hence, some issues towards security are [33]: usability, scalability, threat modelling, key management, quality of management, etc. Some other issues are listed here are:

- Insufficient Privacy Response: The problem is to mould the users' feedback in such a way that the level of abstraction of private details fall way below a certain threshold. The usage proves to be stuck if the service provider fails to provide further information. Instead, the clients may be exposed to a number of messages or will be led to believe that they are still being provided with the services though they are not. The settlement of privacy with application is a rising concern.
- Scalability: A majority of the researches are done on surveyed data which has been obtained from controlled environment, ranging to a smaller area and client population. These models which have been generated in the testing atmosphere have to prove themselves for their scalability when applied to a larger area and client population [34].
- Changing Environment: Client find it easier to be more flexible and move between different computational environments and user interfaces with a number of systems and applications [35]. However, it is to be noted that when the clients move, they expect their data to be commuted as well and hence it poses a challenge for all model designers as they have to create models that emphasise on this mobility.
- Private Information Retrieval: Some applications or users require services without providing or using any user identifiable information. This is a problem similar to domain of Private Information Retrieval (PIR) protocols [1, 6]. This provides data retrieval with queries that require user information without disclosing the same information. Developments of applications that provide PIR have not been given sufficient attention in pervasive computing.
- Avoiding Privacy Violation for Resource Sharing: The presence of clients' information often leads to violation of privacy policies while communication for other sources and services. Designing a model that resolves this issue efficiently is indeed a task to achieve pervasiveness.

B. Privacy issues in Pervasive Computing

In 1991, Mark Weiser already identified privacy in Ubiquitous Computing (ubicomp) as one of its biggest challenges [36]. According to Steffen et al. [38], privacy is "as an entity's ability to control the availability and exposure of information about itself". Broadly speaking, privacy refers to claiming of individuals, groups, etc., to reciprocate when, how, and to what level the details about them are being transferred to others. The umbrella spread of pervasive computing is what makes preserving a user's privacy a herculean task. Compounding spaces with sensors, actuators, etc. results in a construction of innovative area and computational analyses which will be globally accepted. With the help of numerous sensors and embedded systems, the spaces can be easily customized for the clients' interests and can extract the context details completely. Consider the case of intruders invading and exploiting this technique in order to trace certain clients or users. In fact, there are a few situations when people want to be anonymous so that they cannot be tracked by anyone else.

In daily life, with people being surrounded by a bazillion number of smart devices and gadgets, privacy in persistent computing is raised to be a serious issue [22, 26, and 28]. These devices are embedded in artefacts and other articles including human bodies and have skilled communication capabilities, ability to implement spy work, etc. In near future, these questions re likely to pop up in our minds when using our smart devices:

- Can I trust my refrigerator? With the advent in innovation and technology, fridges are likely to report the dietary misbehaviour of its owner to the concerned doctor.
- Can I trust my smart phones, TV, etc.? All smart devices make use of cookies, and other methods to get a better insight into the lives of its owners to customize the product accordingly.
- Will pervasive computing force us to abandon all hope for privacy?
- Will the existence and presence of cyber-flies whose eyes are substituted with high-resolution cameras bring a halt to privacy?
- Would it be clever enough to develop a cyber-spider to decrement the cyber-flies? But cyber-birds would feed on them too.

So, we will build a cyber-cat for overcoming above issues. Will a new privacy category appear/ protecting artificial entities' privacy? Note that socially based paradigms like trust-based approaches will play a big role in pervasive computing in protecting privacy. Privacy and Trust, both are integrated terms in computing environment. Hence, this section discusses several critical issues like security, privacy, etc., in pervasive computing environment. Now next section will discuss respective issues in distributed computing environment.

IX. DISTRIBUTED COMPUTING

Due to recent development in technology like Blockchain, etc., the future belongs to distributed era (environment) [11], for example, distributed computing, distributed network, distributed web, etc. With distributed functionality in a network, user builds more trust among other user [34]. In general, distributed computing is difficult to understand for individuals, i.e., who has data about them, where it is stored, and how it is being used. Ensuring quick and easy access of intense data to the clients can be executed by combining the dissimilar, separate and different computer systems and databases into a single space. However, this also raises the privacy and security concerns which need to be resolved. How is it that the customers can be assured that there will be no breaching of data in a distributed system? How can national privacy and consumer rights be protected across a global grid? How can clients be ensured that their data isn't be used for malicious purposes during transactions with a vendor? How can we prove to the clients that data would remain in loyal jurisdictions? What kinds of redressal methods can be used for a customer's privacy of data? And most importantly, as circulated computing makes it simpler for the collection of details about individuals, how much more of the data may be collected and what are the new ways in which it will be used for?

A. Security issues in Distributed Computing

The secured execution of distributed systems has created a number of severe issues. Few points are listed here as:

a. Identifying the methods which analyse the level of security in a system;
b. Monitoring the system safety;
c. Developing the security metrics;
d. Integrating ideas, like cryptography, etc. for secured and safe conversations;
e. Using middleware in system security;
f. Using web services for enhancing security.

B. Privacy issues in Distributed Computing

There has been an ardent desire for the evolution of computational technology due to recent enhancements in Interne technology. These days' users do not even have to make use of private machines for executing their computational tasks. Simultaneously, there has been an evolution in data storage as well as people have moved to storing data in cloud. This has led to a global acceptance of computation and data analysis with enhanced accessibility and assurance. Together this, advancement in technology has also created several new challenges in distributed computing environment [38], like (issues in distributed computing) are: Trust, Robustness to network delay, Efficiency, Scalability, Threats to validity, and Secure computation.

A distributed computational system contains numerous software parts which function as a single system and hence, it generates a number of golden opportunities for further research. Hence, this section discusses several issues raised in distributed computing. Now, next section will deal with security and privacy concerns with respect to future Internet society.

X. FUTURE INTERNET SOCIETY

Internet has turned out to be the highly used and most required tool of the modern century. Little did we know, that internet would bring about such a drastic evolution seeding grounds for human environment, socio-economic growth, etc. Questions like "What Will the Internet Look Like In 10 Years"? or "How many smart devices will be connected through internet in 2030"? Internet of people, Internet of value, internet of everything, internet of Nano-Things are some enhancement using internet in today's applications. But, here also several issues also raised together popularity of internet which are included here as:

A. Security issues in the Future Internet Society

Internet is the basic backbone for any kind of computing environment/ technology. Some of the security issues related to the future internet are:

- Consistent and real-life supervision and control of security systems, context, services, etc.
- Detection of intrusions and attacks by malicious users at a primitive stage to prevent critical and chronic impairment, analysing and understanding he mannerisms of the harmful model designs in order to produce new schemes and proposals.

- Safeguarding the interrelated frameworks of the modern era against attacks, cascadings, interventions, etc.
- Cross-border, cross-organizational, scalable and well dispensed, co-related security methodologies, including the measures influenced by the bio-spherians: collective and self-made, self-healing and self-studying mechanisms.
- Handling and controlling the "identity" of a huge number of networking citizens, gadgets, services, etc.
- Watching over the communications and interfaces existing between non-uniform ICT (Information and Communications Technology) systems and developing possible security norms across the futuristic net.
- Protecting the key frameworks which are interrelated and are controlled by exhaustive networks.
- Designing systems and services that have high scopes, and those which are dependable and resistive in nature.
- Qualifying security, dependability and resistive nature during design and manufacture or doing it dynamically during run-time.
- Anticipating, supervising and controlling the dependant nature, progress and comforts to the rapidly changing content, conditions, rules, norms, etc. along with a guaranteed service level set up between the contrasting factors.
- Protection of distributed virtual objects and efficient frameworks based on interactions, storage reservoirs, etc.
- New crypto-schemes are introduced in the main networks to deal with the ever-increasing data transfer rates in the modern era.

B. Privacy issues in the Future Internet Society

Through computing devices which are connected with internet network, then information can be accessed from anywhere, anytime (in this smart era). Some of the privacy issues related to the future internet are:

- Comprehending and recreating a personal-friendly identity management scheme;
- Reimbursing privacy and safety in the future environments; new privacy designs and models and data control modules with advancing technologies;
- Frameworks and technical foundations for controlling personal details and for data distribution;
- Analysing the emergence of trust and related terminologies;

In near future, we need to develop novel, trustworthy, reliable, and usable algorithms, which are efficient enough to carry out informed decisions about which information, service and system they can rely on. Hence, this section discusses several critical issues like security, privacy, etc., with respect to Future Internet Society. Now, next section will deal with security and privacy concerns, raised in Grid computing environment.

XI. GRID COMPUTING

Grid computing (or a processing architecture) combines several computers (together) to reach a common objective/ to solve a problem. In lay means words, grid computing is a computer network involving each computerized resource to be shared with every other computer to achieve a major target [4]. Large number of network registration in Grid computing, is a capable and proficient computational innovation. A framework which is registered with grid, is rising as a promising innovation for three reasons: (i) its capacity to make more cost-proficient use of a given measure of figuring assets, (ii) as an approach to tackle substantial scale issues that cannot be unravelled without a remarkable measure of processing force, and (iii) since it recommends that the assets of many PCs can be controlled and directed towards a typical goal. Now some similarities between cloud and grid computing are:

- Scalability: The ability of an efficient system to handle the doubling load of work along with improvisation is called scalability. Grid and cloud are two well versed examples of scalability based on their performance. CPU and network spectrum are directed on command. Hence, grid and cloud networks have a great storage space that is flexible and it depends on the number of users and the collection of data transfer rates at a point.
- Multitenancy and Multitasking: Multitenancy is a case where individual instanced software serves numerous users, while multitasking [4, 8] is the audacity to carry out versatile tasks and share resource. Both are complementary to grid and cloud-based networks and thus, allow users to execute a variety of tasks.

Hence, though cloud computing shows enhancement from grid computing [8], there are numerous similarities under them. Grid computing proves to be better for institutes with bulk data requirements being serviced by small number of users. On the contrary, cloud computing is suitable for those situations where there are multiple users and clients who necessitate small amounts of data alone. Now, some characteristics of Grid Computing over Cloud Computing are: Heterogeneity (grid has different Operating System and Hardware), Loosely coupled (grids are distributed in nature over a network), scattered (grid use many machines but not at a single location), and Resource handling (done by the resource manager at each node as an independent unit), etc. Now, concerns like security, privacy in respective computing technologies can be discussed as:

A. Security issues in Grid Computing

Security can be referred to as the strata which contains resources necessary for grid architecture and design. Security means need to protect something from outside world/ malicious/ unknown users. The resource (in used) may be valuable and protected with weak security mechanisms. The security issues in a grid are sophisticated and the resources are positioned in a number of domains, each having its own norms and rules. In grid computation, we need to protect: Private, anonymous accounts, and Runtime process monitoring.

In summary, security issues in grid computing [3] are: System Security of Server and Database, Networking Security, User Authentication, Data Protection, System and Storage Protection.

B. Privacy issues in Grid Computing

The mobile cloud users have several serious concerns like data security (during data in motion/ at rest or stored), data privacy, etc., in a cloud/ grid enviroenment. Now, some privacy issues related to data (in grid environment) are included as:

i. Risk of data steals and leaks
ii. Data privacy lies in the hands of customers
iii. Violating privacy rights
iv. Lack of physical safety and secureness
v. Dealing with encryption and decryption of keys
vi. Safety issues of virtualised machines
vii. Lower standards for data integrity
viii. Incompatibility of services because of the involvement of too many vendors

Note that privacy issue is raised only when a data/ information (personal or confidential) leak. It is also necessary to encourage the clients to adapt to cloud data services which have distinct standardization. In addition to the data security threats (on cloud/ grid side), some attacks are always possible at end-user mobile devices [4] like Device Data Theft, Virus and Malware Attacks via Wireless Devices and Misuse of Access Rights. On another side, other issues (in grid computing) are: latency, low internet connectivity, location awareness, engagement of maximum system/ machines (for completing main task) or sharing of resources together, architecture related (information sector), infrastructure (host and network) and management issues (credit management, trust management, monitoring). Some resources in a system are useful and taking part in a computation (with other system's resources) but some are useless and not taking any participation in solving a problem, but creating problem, i.e., sending system in deadlock state.

Hence, this section discusses several critical issues like security, privacy, etc., with respect to Grid computing. Now, next section will deal with several security and privacy concerns, raised in Vehicular Ad-hoc Network/ Vehicular Cloud Computing environment.

XII. VEHICULAR AD HOC NETWORK

Vehicular Ad Hoc Network (VANET) is a subset of Mobile Ad Hoc Networks (MANET) [10, 17 and 25] having a few dissimilarities like restriction in power, mobility patterns, etc. In VANET, cars commute as nodes in network for the production of a mobile network. In VANET, vehicles use On Board Units (OBU) and Rode Side Units (RSU) for making communication among each other. For simulation purpose, in VANET every participating vehicle communicates through wireless router, and allowing vehicles to be in range of 100 to 300 metres. In near future, we need to provide efficient services to each and every vehicle (in Future Vehicular Network (FVN)). Basically, VANETs were primarily designed to support the communication between totally different Vehicles (Vehicles to Vehicles: V2V) and infrastructures (Vehicle to Infrastructure: V2I) [25]. During this growing phase of VANET, several issues like security, privacy, and trust, scalability, etc., raised in it. But, among all existing issues (or challenges) of the VANET/ Future Vehicle Network, security, privacy (also trust) received less attention. Each vehicle or service provides contain information about a vehicle user. It is important that this information should not modified by an attacker (including drivers should also respond with full trust, i.e., correctly about traffic management. It is to be keenly noted that the size of the network, geographic relevance, flexibility, etc., makes the execution harder and different from other network protections. Hence, each issue is discussed in detail as:

A. *Security Issues in Future Vehicular Network*

Security and privacy concerns [1] are very similar to majority of the mobile and wireless connection set ups: authorization, data consistency, resilience to future attacks and interventions like Denial of Services (DoS), Sybil attacks, etc.

Issues of security and privacy are nearly common to most mobile and wireless network settings: authentication, data integrity, resistance to various attacks like Denial of Service. Here are a few major differences observed:

- No Confidentiality: This is mainly applicable in the mobile network sector. For example, in the recent cell-phone models (GSM, CDPD, etc.) there is the existence of a secure channel between the phones and the closest base station or registry. The safety and security needs for VANETs are similarly needed in V2V (Vehicle to Vehicle) group interactions. Hence, this is to be taken up as a key issue in the field of VANET.
- No Key Distribution: Prime assortment is a necessity in VANET due to the following two concerns: a) no chances of bulk data being transferred between vehicles or – frameworks b) vehicles which pace with a greater acceleration are likely to be present in the base station for less amount of time within a particular station. It is also to be noted that these vehicles use broadcasting techniques to transmit the data (in a pair/ group) and key distribution is not compulsory. Mobile network architecture has the facility for key dispensing.
- No Hand-Over: When a node commutes from one cell to cell, its state and data are being simultaneously transferred. Same way, in VANET, physical transfer of data is eradicated in the case of handling humongous volume of data, i.e., vehicle which are required to attest their speed and other arguments to the station.
- No Battery Power: On the whole, the power consumption (CPU) is rated high for most of the mobile networks. The power is consumed for receiving and transmitting the data as well as to form cryptographic operations on nearly dead and power challenged gadgets including PDAs, mobile phones, etc.
- No CPU Speed: Reduced CPU speed of the nodes is of prime concern in many of the mobile networks. Security and safety norms are managed to reduce cryptography.
- Extreme Time Sensitivity: Time management proves to be another essential factor for which we can rely on CPS devices for accurate and precise clock measurements. After all, the devices must be prejudices of replays and else unreceptive. It is easier to access simpler frameworks embedded with features like digitalised signs, certified framework, etc.

Now, some serious privacy issues will be discussed as our next task of this section.

B. *Privacy Issues in a Future Vehicular Network*

Note that why is Privacy Important for VANETs? To give answer to this question, we need to discuss some threats to the privacy, which have investigated/ measured in the past decade. Here, leaking of traces/ information can be represented in terms of degree/ level. The levels and different tiers of privacy determine the aim and targets of the system on the basis of which privacy would have to be finally designed. Here are a few examples to overcome the hurdle of future privacy:

- To analyse the mannerisms of the driver during the driving session so that the gained details can be of use to the police as well. In case of over-speeding, penalty tickets can be issued to the concerned person.
- Parking areas can be efficiently managed by making use of car identifiers to capture any form of communications taking place in the parking which would act as an upper-hand to retrieve the arrival and departure information regarding any personnel.
- By detecting the cars' movements and behaviours, fines can be easily issued for any form of misconduct or other acts.

Moreover this, many attempts have tried in previous decade for preserving user's privacy in [15, 16, 23, 24, and 25]. Though these principles are in agreement with mislinkage's and intrackability principles, privacy ought to be considered for data sharing. Specifically, positional information can be made use of to track a vehicle, though its aliases are in use. It is also important to provide minimalized details to the remaining vehicles, while maintaining its worthiness.

- Location cloaking techniques: In order to compensate for the trade-off, these techniques have been issued because of which, positional details and information will be portrayed on the achievable of protection and safety.
- Aggregation: It permits the transfer of only segregated and required data, allowing the minimisation of the personal data being sent.
- Non-Repudiation: It targets towards dodging any one particular instance after having an action performed. For example, the interrelated information in a computerised network may be of NRO: Non-repudiation of Origin, NRR: Non-repudiation of Receipt format. However, NRO's are used more commonly that VANET.

Some popular attacks in VANET [10, 17] are: Message replay attack, Message spoofing, Denial of Service (DoS) attack, Movement tracking. On another side in VANETs, some challenges (related to security) are: Network Volatility, Liability vs. Privacy, Delay-Sensitive Applications, Network Scale, Heterogeneity, Infrastructure less, Multi-hop connection, Wireless Link use. Some other issues (in VANET) are: Availability, DoS and uncollaborative behavior prevention, information trust. Note that in FVN, power consumption is not important since a running vehicle provides an ample source of battery power. Hence, this section discusses several critical issues like security, privacy, etc., in VANET. Now, next section will deal with several security and privacy concerns, identified in location-based services.

XIII. Location Based Services

All vehicles embedded with the location tracking devices like Global Positioning System (GPS) receivers, and other interaction abilities are efficient enough to enable and activate a certain range of location-based applications (like Location Based Services (LBSs)) [1]. In LBSs, users submit queries along with his/ her location to a service provider like "Where is the nearest car parking?" "Where is the nearest Coffee Shop"? Note that, user send these queries together with the geographic coordinate of his/ her current location.

A. *Security issues in Location Based Services*

- What are the norms vested on institutions with respect to the bulk amounts of data they deal with?
- Are the LBS electronic systems well secured and grounded from other attacks?
- What measures have been taken up to control the LBS users?
- Are there any strong back-up measures that have been adopted in case of a system failure?

B. *Privacy issues in Location Based Services*

Preserving Privacy is still impossible as perfectly till communication takes place among human being. The term is said to comprise of the perspectives of information security and safety, discretion during communications and conversations, along with regional secrecy as per Privacy International. Several definitions of privacy can be found in [1, 6]. Here, some categories of privacy are; "privacy of the person," "privacy of personal behavior," "privacy of personal communications," and "privacy of personal data." It is an oblivious fact that secrecy and human beings would always go hand in hand with each other. It is leads people to live a life of their own by keeping their thoughts, interests, likes, etc., to themselves. Secrets are often considered to be a mechanistic and holistic way of protection, which is ardent for self-perseverance and thereby, necessary for preserving security. As an individual, it is known to all of us that we need to preserve our secrets and mask them from the raging world. Even so, we seem to be discomforted by the secrets which are possessed by the government. Secrets can be of different types. For example, when secrecy is being used to protect the national interests, it is invulnerable. Everything is secret, nothing is secret for a human being [1]. No one care much about his/ her privacy, but it matters or everyone cares when he/ she is being tracked for a period of time continuously. The best way to ensure that keep secrecy of users as most important secrets, kept as secret (with a higher trust), is for secrecy to be returned to its limited but necessary role.

- Who is permitted to access the positional details?
- Can individual possess tracking devices which may be deactivated?
- Are the benefits from LBS in a given context known to overweigh the effects of personal privacy invasion?
- Is the privacy of an individual way higher when compared to the safety and personal deeds of the community?

With rapidly increasing wireless and mobile technologies, LBSs are being exposed to security and personal safety breaches. Privacy can be defined as "the secretive technique of masking ones' current position from those of another [1, 6]. Locational privacy is of utmost concern when compared to all of the other LBS categories as it reveals all of their personal traits and figures including their addresses, hobbies, etc. Privacy can be further turned into data, location, identity and genomic. Some privacy issues existing in location-based services is included as:

a) Should the user whose location is being tracked be informed when in use? Can they be granted permission to switch it off? What factors may influence these responses?
b) Should the user be allowed to handle the collection of location information?

c) Can the positional information be identified individually, or can the user decide on the levels of anonymity it possesses?
d) What type of preservance can a persons' past locational information have against search and captivism?
e) Should it be allowed to govern other perspectives of stored details like accuracy, levels of safety, etc.?
f) Does usage of native details be another middleman like carriers create an atmosphere of unfair advantage for malicious use of information?
g) Up to what proximity should the users be permitted to choose their own degrees of anonymity?
h) What levels of exposure can be efficiently handled by the government?
i) What are the regulations and norms which are rightly put together to assure rights of privacy to the citizens?
j) Will the unparliamentary standards along with industries/trade groups be strict enough to be effectively accepted by consumers and industries?
k) Would the public interest groups be sufficient for monitoring the industries and safe guarding the public interests?
l) Will the demands be satisfied by the providers corresponding to their respective features, products and services?

Some of the other Privacy and Security issues in LBSs have been discussed by the Tyagi, A.K and N. Sreenath in [1, 6]. Hence, this section discusses several serious issues like security, privacy, etc., in LBSs. Now, next section will identify some security and privacy concerns in Blockchain technology concept (especially used for building trust).

XIV. BLOCKCHAIN TECHNOLOGY

Blockchain is a new technology developed to build trust among users, decentralized and distributed in nature. Popular example of Blockchain based in Bit coin, a cryptocurrency launched in 2009 [29]. In spite of the generic use of Blockchain techniques, it possesses a number of threats. Here are a few major challenges which have been commonly found:

A. *Security Issues of the Blockchain Technology*

Security proves to be the topmost attractive feature of a Blockchain technology and it is completely founded on the basis of public ledger and distributed consensus [11, 29]. However, fraudulent issues and hacking are still prevalent. 51% attack, where in a Bitcoin is made use of for assessing the computational measures with respect to the hash rate, is a frequently observed one. When hash rate is managed by more than 51% of an individual node or a pool of miners, blockchains are vulnerable to malicious acts, thus leading to a fork, i.e., when there's a presence of two contradicting blocks. A great chunk of the mining power has to complement the attackers' block which would further be sent to the Blockchain. Double-spending attack is a very well-known security issue [39, 40, AND 42] and it easily occurs a large number of people make use of the same body to pay their funds (cryptocurrencies like bitcoin [29]). This is made fruitful in a Peer to Peer network as there are high chances of processing delays when the remaining payments are published in a distributed manner to the nodes in the network. Miners require only ten minutes to obtain the solution of the problem. So, these issues are the necessary and efficient solutions to overcome the hurdles with a popular mechanism

B. *Privacy Leakage*

Public and private keys can be used to preserve a definite amount of privacy through Blockchains and the users easily operate on the keys anonymously. However, it has been discussed in [11, 40] and is very clear that Blockchain will never assure transactional privacy as the values of all transactions and payment history for each key will be publicly visible. Moreover, in [40, 41], authors have portrayed how a users' bitcoin transactions and payment accounts can be related to reveal the users' personal details. Furthermore, Biryukov et al. [11] presented a methodology to connect user ids to the IP addresses in spite of the users being masked behind the Network Address Translation (NAT)/ firewalls. In this work, they showcase that each individual client need to be distinctly identified by the node set it is connected to which can be apprehended and used to find the point of origin if a transaction.

Moreover this, multiple methods like Mixing, Anonymous, etc., have been proposed to improve anonymity of Blockchain, but none of the approaches work sufficiently. Hence, this section discusses several issues like security, privacy in Blockchain technology. Now, next section will conclude this work in brief with some suggestions, necessary for future computing environment.

XV. CONCLUSIONS

Security, i.e., the secrecy, uprightness, and validness of data are frequently a vital fixing to protection, as it encourages the control of data streams (i.e., who becomes acquainted with what when?) and guarantees the accuracy of information. It is conceivable to have abnormal amounts of security yet no protection (think observation state), or even some kind of security without security (e.g., a private table discussion in a Taj Hotel). The imperative knowledge is that just actualizing some type of security is insufficient to guarantee protection. Guaranteeing the classification and genuineness of a specific data does not say anything in regards to how and when this specific bit of data will be utilized by its assigned beneficiary. Security of a calculation used to signify "the PC running the calculation ought to be shielded from pernicious bargain", and protection of information used to infer unapproved substances could not access that information. Several scientists/ researchers have proposed several mechanisms to overcome above discussed issues. In last, meaning and importance of security, privacy and trust is troublesome. Protection is identified with, however not indistinguishable with: mystery, isolation, freedom, self-rule, flexibility, closeness, and personhood. Protection is a non-monotonic capacity and social process. Security, Privacy and Trust are easy to lose, but yet difficult to rebuild/ protect. Note that e-healthcare/ Medicare or healthcare sector faces several security, privacy and trust issues in today's smart era [43]. Because of the recent advancement of systems administration and interchanges innovations and its open nature, today's security, protection and trust has gotten to be significant issues. Everybody require security and assurance from assailants, i.e., require dependable connections. As future work, we want to provide reliable experiences/ services to human beings (as an extended version of carpooling where drivers allow passengers to dictate their priorities). So, everybody is heartily welcomed to extend their research in this field.

Acknowledgment

This Research is Funded by Anumit Academy's Research and Innovation Network (AARIN), India. The Author Would Like To Thank AARIN, India, a Research Network For Supporting The Project Through Its Financial Assistance.

References

[1] Amit Kumar Tyagi, Sreenath N., "Future challenging issues in location based services", International Journal of Computer Applications, Vol. 114 (5), 2015.

[2] Abid Shahzad1 and Mureed Hussain, "Security Issues and Challenges of Mobile Cloud Computing", International Journal of Grid and Distributed Computing Vol.6, No.6, pp. 37-50, 2013.

[3] Muhammad Asif Habib and Michael Thomas Krieger, "Security in Grid Computing" (http://www.fim.uni-linz.ac.at/lva/SE_Netzwerke_und_Sicherheit_Comm_Infrastructure/gridcomputing.pdf)

[4] Anirban Chakrabarti, Grid Computing Security, book, ACM, 2007.

[5] Buyya, Rajkumar & Broberg, J. & Goscinski, Andrzej. (2011). Cloud Computing: Principles and Paradigms. 10.1002/9780470940105.

[6] Amit Kumar Tyagi, N. Sreenath, "A Comparative Study on Privacy Preserving Techniques for Location Based Services", BJMCS, July, 2015 10(4), pp. 1-25, 2015.

[7] B.David "3 security risks posed by the Internet of Everything" (https://www.federaltimes.com/opinions/2015/03/10/3-security-risks-posed-by-the-internet-of-everything/) Mar, 2015.

[8] Rajendra Kumar Dwivedi, "From Grid Computing to Cloud Computing & Security Issues in Cloud Computing", TECHNIA – International Journal of Computing Science and Communication Technologies, Vol.5 No. 1, July 2012 (ISSN 0974-3375).

[9] T.Kavitha and D.Sridharan ," Security Vulnerabilities in wireless sensor networks : A survey," Journal of Information Assurance and security , Vol.5 2010.

[10] Amit Kumar Tyagi, N. Sreenath, R Priya "Never Trust Anyone: Trust-Privacy Trade-Offs in Vehicular Ad hoc Network", British Journal of Mathematics and Computer Science (BJMCS), Vol. 19, No. 6, pp. 1-23, November 2016.

[11] Biryukov, Alex & Khovratovich, Dmitry & Pustogarov, Ivan. (2014). Deanonymisation of Clients in Bitcoin P2P Network. Proceedings of the ACM Conference on Computer and Communications Security. 10.1145/2660267.2660379

[12] Tyagi, Amit & Krishna, A. & Malik, Shaveta & Nair, Meghna & Niladhuri, Sreenath. (2020). Trust and Reputation Mechanisms in Vehicular Ad-Hoc Networks: A Systematic Review. Advances in Science, Technology and Engineering Systems Journal. 5. 387-402. 10.25046/aj050150.

[13] Diebold, Francis. (2012). On the Origin(s) and Development of the Term 'Big Data'. SSRN Electronic Journal. 10.2139/ssrn.2152421.

[14] Amit Kumar Tyagi, Meghna N Nair, and N.Sreenath, "Where Is Current Research on Big data?— A Systematic Review", IJICIC (Communicated).

[15] L. Sweeney.k-anonymity: a model for protecting privacy.International Journal on Uncertainty, Fuzziness and Knowledge-based Systems,10 (5), 2002; 557-570

[16] Machanavajjhala, Ashwin & Gehrke, Johannes & Kifer, Daniel & Venkitasubramaniam, Muthurama krishnan. (2006). l-Diversity: Privacy Beyond k-Anonymity. ACM Transactions on Knowledge Discovery From Data - TKDD. 1. 24. 10.1145/1217299.1217300.

[17] Amit Kumar Tyagi, N. Sreenath, "Providing Trust Enabled Services in Vehicular Cloud Computing (extended version)", 25-26 August, 2016, in proceeding of ACM/ International Conference on Informatics and Analytics (ICIA), Pondicherry, India, pp. 1-10.

[18] W.Brujin, M.Spruit and M.Heuvel, " Iddentifying the cost of security", Journal of Information Assurance and Security , Vol.5, 2010.

[19] Kevin Ashton, That 'Internet of Things' Thing. RFID Journal, June 22, 2009.

[20] Tyagi, Amit Kumar and Sharma, Sonam and Anuradh, Nandula and Sreenath, N. and G, Rekha, How a User will Look the Connections of Internet of Things Devices?: A Smarter Look of Smarter Environment (March 11, 2019). Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE) 2019.

[21] P P Ray, A survey on Internet of Things architectures, Journal of King Saud University - Computer and Information Sciences, Volume 30, Issue 3, July 2018, Pages 291-319

[22] Tyagi, Amit & Rekha, Gillala & Sreenath, N.. (2020). Beyond the Hype: Internet of Things Concepts, Security and Privacy Concerns. 10.1007/978-3-030-24322-7_50.

[23] N. Li, T. Li and S. Venkatasubramanian, "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity," 2007 IEEE 23rd International Conference on Data Engineering, Istanbul, 2007, pp. 106-115.

[24] T. M. Truta and B. Vinay, "Privacy Protection: p-Sensitive k-Anonymity Property," 22nd International Conference on Data Engineering Workshops (ICDEW'06), Atlanta, GA, USA, 2006, pp. 94-94.

[25] Tyagi, Amit & Sreenath, N.. (2015). Preserving Location Privacy in Location Based Services against Sybil Attacks. International Journal of Security and Its Applications. 9. 175-196.

[26] Tyagi, Amit Kumar and M, Shamila, Spy in the Crowd: How User's Privacy Is Getting Affected with the Integration of Internet of Thing's Devices (March 20, 2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India, February 26-28, 2019.

[27] CISCO – IoE report, https://www.cisco.com/c/dam/global/en_my/assets/ciscoinnovate/pdfs/IoE.pdf

[28] Sravanthi Reddy, Kavita Agarwal and Amit Kumar Tyagi, "Beyond Things: A Systematic Study of Internet of Everything", Internet of Things, 16-18 December 2019, in Proceeding of Springer/ 8th World Congress on Information and Communication Technologies, GIET University, Odisha, India.

[29] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008

[30] Rekha G., Tyagi A.K., Anuradha N. (2020) Integration of Fog Computing and Internet of Things: An Useful Overview. In: Singh P., Kar A., Singh Y., Kolekar M., Tanwar S. (eds) Proceedings of ICRIC 2019. Lecture Notes in Electrical Engineering, vol 597. Springer, Cham

[31] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proceedings of the 2012 ACM first edition of the MCC workshop on Mobile cloud computing.ACM,2012, pp. 13–16.

[32] M. Aazam and E.-N. Huh, "Dynamic resource provisioning through fog micro datacenter," in Proceedings of the 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops). IEEE, 2015, pp. 105–110.

[33] Ahamed, Sheikh, Security in Pervasive Computing: Current Status and Open Issues. International Journal of Network Security, 2006.

[34] Ivanović, M., Vidaković, M., Budimac, Z. et al. A scalable distributed architecture for client and server-side software agents. Vietnam J Comput Sci 4, 127–137 (2017). https://doi.org/10.1007/s40595-016-0083-z.

[35] M.Fowler, "Patterns of Enterprise Application Architecture Addison Wesley, 2002. ISBN: 978-0-321-12742-6.

[36] Weiser, Mark: The Computer for the 21st Century. Scientific American 265(3), pp. 94-104, September 1991.

[37] Steffen, S., Bharat, B., Leszek, L., Arnon, R., Marianne, W., Morris, S., et al., (2004) "The pudding of trust". IEEE Intelligent Systems, 19(5), pp. 74-88.

[38] Steen, M.V., Pierre, G., & Voulgaris, S. (2011). Challenges in very large distributed systems. Journal of Internet Services and Applications, 3, pp. 59-66.

[39] A Mohan Krishna and Amit Kumar Tyagi, "Intrusion Detection in Intelligent Transportation System and its Applications using Blockchain Technology", 24-25 February 2020, in Proceeding of IEEE/ International Conference on Emerging Trends in Information Technology and Engineering, VIT Vellore, Tamilandu, India.

[40] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and Privacy on Blockchain. ACM Comput. Surv. 52, 3, Article 51 (July 2019), 34 pages. DOI:https://doi.org/10.1145/3316481

[41] Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE 11(10): e0163477. https://doi.org/10.1371/journal.pone.0163477

[42] Bruno Tavares, Filipe Figueiredo Correia, and Andre Restivo, A survey on Blockchain technologies and research, Journal of Information Assurance and Security, (JIAS), ISSN 1554-1010 Volume 14 (2019) pp. 118-128.

[43] Joao Pedro Dias, Angelo Martins, and Hugo Sereno Ferreira, A Blockchain-based Approach for Access Control in eHealth Scenarios, Journal of Information Assurance and Security (JIAS). ISSN 1554-1010 Volume 13 (2018) pp. 125-136.

Authors Biographies

Amit Kumar Tyagi is Assistant Professor (Senior Grade), and Senior Researcher at Vellore Institute of Technology (VIT), Chennai Campus, India. His current research focuses on Machine Learning with Big data, Blockchain Technology, Data Science, Cyber Physical Systems, and Smart and Secure Computing, Privacy). He has contributed to several projects such as "AARIN" and "P3-Block" to address some of the open issues related to the privacy breaches in Vehicular Applications (like Parking) and Medical Cyber Physical Systems. He received his Ph.D. Degree from Pondicherry Central University, India. He is a member of the IEEE.

Meghna Manoj Nair is a student currently pursuing B.Tech course in Computer Science and Engineering at VIT Chennai. Venturing into completely different aspects in the field of Computer Science and following a plethora of other incorporations with respect to Artificial Intelligence, Machine Learning, Blockchain, Robotics, etc. which glamorizes and enhances the existing developments is one of the things She is passionate about. She has also had golden opportunities to share her bit of work to some of the trending research topics which include Cyber Physical Systems, Blockchain, Deep Learning etc. under the guidance of Dr. Amit Kumar Tyagi.

Dr. Niladhuri Sreenath is a Professor in Computer Science and Information Technology at Pondicherry Engineering College affiliated to Pondicherry University. He obtained my Ph. D. in Computer Science from Indian Institute of Technology, Madras under the guidance of Prof. C. Siva Ram Murthy. His primary research interest lies in WDM Optical Networks, Privacy and Trust.

Dr. Abraham is the Director of Machine Intelligence Research Labs (MIR Labs), a Not-for-Profit Scientific Network for Innovation and Research Excellence connecting Industry and Academia. As an Investigator / Co-Investigator, he has won research grants worth over 100+ Million US$ from Australia, USA, EU, Italy, Czech Republic, France, Malaysia and China. Dr. Abraham works in a multi-disciplinary environment involving machine intelligence, cyber-physical systems, Internet of things, network security, sensor networks, Web intelligence, Web services, data mining and applied to various real world problems. In these areas he has authored / coauthored more than 1,300+ research publications out of which there are 100+ books covering various aspects of Computer Science. One of his books was translated to Japanese and few other articles were translated to Russian and Chinese. About 1000+ publications are indexed by Scopus and over 800 are indexed by Thomson ISI Web of Science. Dr. Abraham has more than 37,000+ academic citations (h-index of 90 as per google scholar). He has given more than 100 plenary lectures and conference tutorials (in 20+ countries). Since 2008, Dr. Abraham is the

Chair of IEEE Systems Man and Cybernetics Society Technical Committee on Soft Computing (which has over 200+ members) and served as a Distinguished Lecturer of IEEE Computer Society representing Europe (2011-2013). Currently Dr. Abraham is the editor-in-chief of Engineering Applications of Artificial Intelligence (EAAI) and serves/served the editorial board of over 15 International Journals indexed by Thomson ISI. Dr. Abraham received Ph.D. degree in Computer Science from Monash University, Melbourne, Australia (2001) and a Master of Science Degree from Nanyang Technological University, Singapore (1998).