Internet of Things: Security Perspective Survey

Chirantar Nalawade, Piyush Rumao

Abstract: As the communications becoming faster and faster, computing power becoming cheaper world sets its foot in new era of computing technology, Internet of things which involves connection of billions of cyber-physical systems overcoming their complexity and heterogeneity is near future. Although internet of things will makes lives smarter with various concepts such as smart cities, security and privacy of such a huge network will be a big issue. Security and privacy are major areas of internet of thing structure which needs to be carefully addressed and resolved so that human lives are prevented from various threats and vulnerabilities. Although lots of research is going on internet of things, it will be important to note down various fact and data which will be helpful for guiding the futuristic research. This paper carries a survey on various important topics in internet of things security such as threats and attacks, architecture, privacy issues, data security, physical layer security models, communication technologies and security issues relative to cloud.

Index Terms: Internet of Things, Threats and attacks, Architecture, Data security, Data Privacy, Communication layer security, physical layer security methods.

1 INTRODUCTION

Have you ever imagined a state where your health insurance company gets to know whether you have more fast food stored in your refrigerator than healthy food? Yes this sounds very much possible in the near Future with the age of Internet of Things (IOT) soon blooming up and every single item will be having thousands of sensor chips connected to the internet monitoring your minute data at every fraction of seconds. Well that sounds fascinating , but it comes with a serious side effect where sinister organizations will be ready to invest in millions to hack your devices connected to the internet and get potential useful information as per business needs so that they adopt a right policy to target potential customers, well such spying is acceptable to some extent but what if that compromised information happens to be your private data say bank statements, salary information, personal relationships or anything that you don't want the outsider to know.

Stopping the rise of IOT is not a solution, so why not think of making privacy protocols to secure it. That's where our survey paper come into picture where we have taken various parts of IOT and talked about the potential threats it is likely to face and plausible solutions or future research which need to be carried out in that area to secure a loophole.

This survey paper is targeted at wide audience which includes information security researchers, chief information officers, technological consultants, security auditors, developers and so on. This paper gives reader crucial insights on major security topics and present a direction in which future research needs to be taken.

To address security as whole, paper breaks security into various sub-domains which are stated next. Section 2 presents various possible threats and attacks on IOT, section 3 focuses on IOT architecture, section 4 describes about IOT privacy, section 5 focuses on physical layer security models, section 6 describes IOT communication technologies, section 6 focuses on data security and section 7 presents focuses on unexplored cloud computing issues perspective to IOT.

2 RELATED WORK AND CURRENT TECHNOLOGIES

J D Santos, C Hennebert, C Lauradoux[1] have demonstrated information leakage occurring even after deploying different levels of security measures in IOT networks. They have demonstrated it using zigbee module and proposed certain countermeasures to it. R V Rao, K. Selvamani [2] signifies the increasing domination of cloud storage and various service providers like IBM, Amazon and Microsoft providing its infrastructure for cloud services. However, security is a major concern in transmitting data to this remote server over internet and authors have highlighted various data security challenges. In Amitav Mukherjee [4] presents an overview of low-complexity physical-layer security schemes that are suitable for the IOT. They even pin point the most energy-efficient and low-complexity security techniques that are best suited for IOT sensing applications.Akshay S. Nagdive, Piyush K. Ingole [5] bring forth a major issue which IOT applications are likely to face in future i.e. large amount of data transmission through wireless sensors. So they have proposed a new technique of Hybrid Compressive Sensing (CS) to minimize the number of data transmissions and balance of the traffic load throughout networks. Madhumita Panda [6] figures out that as Wireless sensor networks (WSN) continue to grow, they become vulnerable to attacks and hence the need for effective security mechanisms. Thus author have tried to identify suitable cryptographic algorithm for wireless sensor network and have implemented the Advanced Encryption Standard (AES) algorithm for providing security in WSN. In J Singh, T Pasquier and others [9] have focused on security considerations for IOT from the perspectives of cloud tenants, end-users and cloud providers, in the context of wide-scale IOT proliferation, working across the range of IOT technologies. They have analyzed the current state of cloud-

supported IOT to make explicit the security considerations that require further work.

3 THREATS AND ATTACKS ON INTERNET OF THINGS

As IOT attracts both maker and hacker it is important to know to know various threats and attacks which can be performed on IOT. Since IOT consists of billions of connected devices and provides with excessive functionality it also takes attack complexity and its types to a next level completely. Also effects of attack on IOT is much severe than common network based attacks such as SQL Injection, Session Hijacking on current Internet Technologies. As a result, we must protect the system from wide range of attacks and threats so that privacy and security are well established. We will list various attacks in 3 major types of attacks namely Phase, Architecture, Network Centrality [1].

3.1 Phase Attacks: Various attacks which are carried on 5 major-phases of Internet of things which are:-

Data leakage and Data breach are types of internal attacks when unauthorized data is exported to unintended location by dishonest employee. Data leakage happens generally when data moves between clouds or various tenants. Data Sovereignty refers to data liability to various laws in which data is stored. Data authentication refers to illegal access of data [1].

Storage Attacks try to disrupt 3 triads of data security i.e. data availability, data integrity, data confidentiality. Denial of service attacks affect availability of attacks. Denial of Service attacks can be created by both legitimate users by flash crowding or attackers by spoofing i.e. sending large no of requests in very short span of time [1].

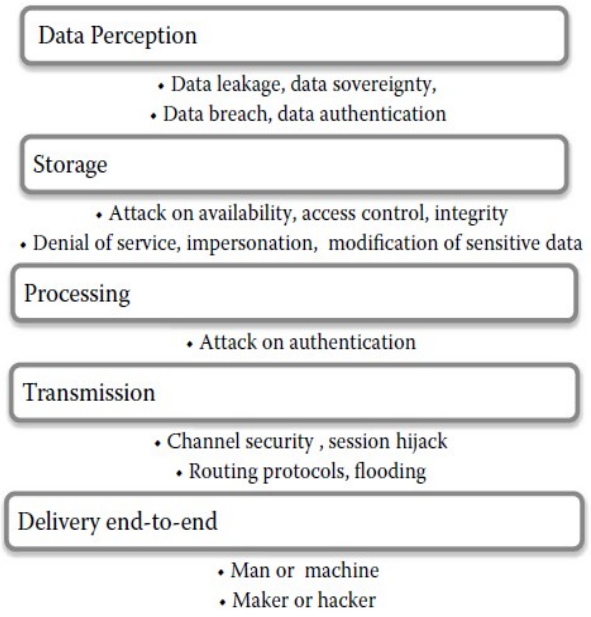

Fig 1: Attacks on 5 Phases of Internet of Things

3.2 Attacks Based on Architecture: Although IOT is not yet confined to well-defined architecture, various attacks can be performed on 4 stages of IOT architecture.

External Attacks are caused by cloud service provider when there is a lack of trustworthiness. As a result sensitive data may be used by malicious organization leading to total comprise in data security.

Worm-hole attacks are famous type of attacks performed in wireless ad-hoc networks where communication medium is radio. Attacker can easily intercept transmission without comprising any of the nodes and is thus to able to inject artificial noise or retransmission may occur [1]. Selective forwarding attack is carried when certain pattern of packets are dropped by malicious nodes while rest are allowed. It results in loss of sensitive data and data integrity is compromised [1].

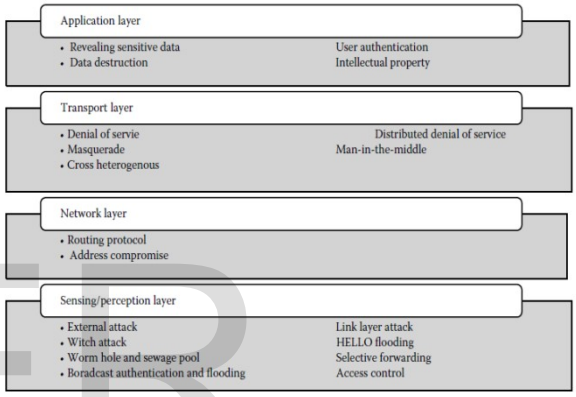

Fig 2 shows various attacks based on architecture.

A witch attack tries to fail a legitimate node thus allowing all the data to pass through malicious node as a result of link diversion. Hello Flood attacks are performed by continuous broadcasting of HELLO messages to all neighbors [1]. As a result legitimate node is unable to obtain the needed resources. Address Compromise is done by making use of IP spoofing attack so that attacks are not filtered by IDP as each attacks has its own unique IP address [1]. Man in the Middle or replay attacks aims to hack system's resources by saving messages and resending them back at a later time [1]. Sybil Attack is carried out on application layer by impersonation of malicious nodes which has acquired multiple identities to prove it as legitimate user. Sybil Attack results in failure of authentication leading to privileges [1]. Attacks based on Network Centrality:-

Node centrality is measure of importance of a node to a network. Centrality attacks disable certain specific target nodes that lead to failure of entire network .Node centrality is measured by 2 main factors i.e. global centrality and local centrality. Global Centrality needs complete network topological information while local centrality needs partial information from neighboring nodes. Attacker can use following methods for calculating node centrality [1].

1. Betweenness: It measures centrality on basis of fractions of shortest paths passing through a node relative to total shortest paths available in the network.
2. Closeness: It measures centrality from perspective of summation of shortest paths from a node to all other nodes.
3. Eigen Centrality: It measures centrality by making use of Eigenvector and adjacency matrix. As a result complete topological information is needed.
4. Degree: It is measure of total no of adjacent nodes.
5. Ego Centrality: It's also called as localized Betweenness as it computes the shortest paths fraction by making use of adjacency matrix.
6. Local Fielder Vector Compatibility (LFCV): It makes of Fielder Vector and distributed power iteration method to calculate node centrality. It denotes importance of a node to overall connectivity.

Effects of Centrality Attacks are measured by feature of node centrality which is no of nodes needed to be removed for bringing largest component size to around 10%.

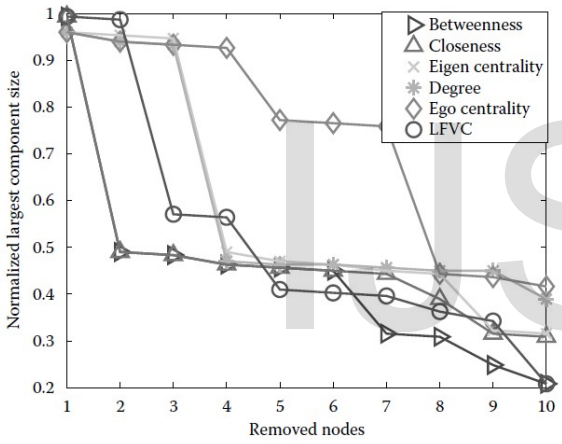

Fig 3:On basis of network resilience of the Europe Internet backbone network topology (GTS-CE dataset), it has been found that Betweenness and LFCV attacks are able to reduce largest component size to 20% by removing 10 nodes and thus are most effective ways.

4 IMPLEMENTATION OF HYBRID APPROACH

Since current cloud and networking technologies and their protocols are limited, it is important to find a new architecture model that will address all futuristic scenarios while capable of providing security and privacy. Nova Genesis (NG) is one of important paradigms that points at integrating many futuristic Internet components to convergent information architecture (CIA).As shown in Fig 4, CIA is able to encompass both intra-node processing which is done by operating system and cloud architecture and inter-node processing of Internet Architecture into a single design system [1].NG architecture addresses following 4 key issues which are backbone of Internet of Things Functionalities.

Naming and name resolution: Current Internet architecture doesn't support unique identification of things and name resolution is limited to domain name system (DNS). As a result Internet architecture is unable to provide name based routing, named service channeling, in-network caching. Service-centric networking and information centric networking put naming at the core of Internet of Things Architecture. To address this issue NG uses natural language naming and self-verifying naming systems (SVN). SVN's are created by making use of immutable attributes which makes objects to have same SVNs in whole networks. There is a loss of traceability which happens in Internet architecture when host moves from one place to another resulting in change of IP address causing a change in identity of host.NG architecture prevents loss of traceability since host remains with a same SVN in whole network. Also Natural language names facilitate search and discovery of service-accesspoints. Since NG services maintain service contracts that are bound to entities SVN, reputation of objects is at stake [1].

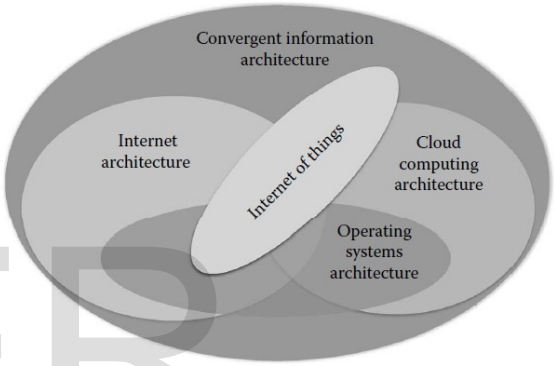

Fig 4: Convergent Information architecture scheme.

Identifier and locator splitting: Since Internet of Things will involve large no of moving devices, identity of host should remain constant even if its location changes. In Internet Architecture, IP address changes when a host moves from one place to another resulting in change of identity. NG addresses this problem by identity/location splitting which enables devices to maintain same identity even if they are in a transit. Unique identity is provided by making use of SVN's which are globally unique and doesn't depend on network topology. Fig 5 shows comparison of Internet Architecture with NG architecture.

Resources, Devices and Content Orchestration: Internet Architecture fails to support large no of devices and control and management of services with physical resources. In NG architecture, a service publishes its name in form of bindings to various other services thereby enabling relationships between resources, devices and their contents. This also leads to social behavior of devices enabling ability to establish trustable relationships and various service level agreements (SLAs) by discovering peers in addition to unique identification [1].

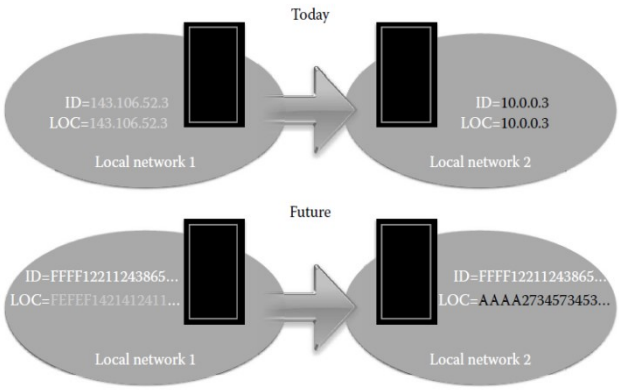

Fig 5: Location/ID gets split in Future IOT architecture whereas it's same in current Internet Architecture.

SLAs lead to joint orchestration of physical resources, devices and enables makes the overall process automatic. Use of reputation services (RpSs) assures a secure and quality service by evaluating reputation of each service before SLA is formed. As a result, good service continues to prosper while bad services are suspended thus mitigating various threats. NG architecture also has a native support of distributed system along with modified proxy/gateway services which is adequate for providing scalability with heterogeneity of IOT platform, protocols and device implementation. This results in proper tuning of Quality of Services, Energy constraints in an IOT system. Intensive research is on-going for need of proper mapping of SVNs to entities so that NG abstractions are properly mapped and physical world resources are securely exposed when required [1].KEY security features of NG architecture

1. SVNs as previously stated provides with lots of security feature such as unique entity identification, data integrity, secured forwarding/routing.
2. Protection against internal threats as it makes use of Pub/Sub communication model which with help of SLA throws current "Receiver accepts all" paradigm to enable efficient utilization of channel resources.
3. Contract based SLAs along with representative SLAs provide ability of forming of trusted networks along with policy enforcements and other constraints [1].
4. Pub/Sub model along SLA-based syncing creates system that favors distributed system architecture enabling use of highly secured Public Key Infrastructure and other distributed key asymmetric cryptographic techniques [1].
5. Use of SLAs lead to unbiased contract and trust evaluation reputation which leads to increase in overall reliability and risk mitigation [1].
6. SVNs enable to identify malicious modifications in an entity since deterministic compilation changes the SVN if the data/code is changed maliciously.
7. Social behavior of devices ensure the ability of finding out malicious devices and their illegal services indirectly paving a way for building critical immunological system to stop spread of malware and mitigate other threats [1].

5 Privacy Issues in Internet of Things

Researchers have found out several vulnerabilities in such IOT entities and the recent example is of Wi-Fi enabled light bulb that allowed them to request its Wi-Fi credentials and use those authentication and authorizations digital certificates to gain network access [5]. Let us have a look at key privacy challenges, solutions and algorithms for privacy of IOT.

A] Key Privacy challenges of IOT:i] Lack of control and information asymmetry [1]. ii] Quality of the user's content [1]. iii] Limitation on the possibility of remaining anonymous when using certain services. iv] Lack of transparency provided by different organization leading to suspicion rising in user about the use of their personal sensitive information [4]. v] Government rules and policies leading to scanning of data and information [1].

C] Algorithms Implemented:-

FP7 is the short name for the Seventh Framework Program for Research and Technological Development. Section map of FP7 projects in the cluster provides a mapping of the FP7 projects deliverables and results against, Governance, security and privacy [12]. Let us have a brief look at each project contributing to ACO5 cluster under FP7 as follows

1) ICORE: This cognitive framework is based on the principle that any real world object and any digital object that is available, accessible, observable or controllable can have a virtual representation in the "Internet of Things", which is called Virtual Object (VO).
2) BUTLER: The goal of the BUTLER project is the creation of an experimental technical platform to support the development of the Internet of Things. The vision behind BUTLER is that of a ubiquitous Internet of Things, affecting several domains of our lives (health, energy, transports, cities, homes, shopping and business) all at once.
3) GAMBAS: The GAMBAS project develops an adaptive middleware to enable the privacy-preserving and automated utilization of behavior-driven services that adapt autonomously to the context of users. In contrast to today's mobile information access, which is primarily realized by on-demand searches via mobile browsers or via mobile apps, the middleware envisioned by GAMBAS enables proactive access to the right information at the right point in time.
4) COMPOSE: Main goal of the Collaborative Open Market to Place Objects at your Service is to simplify the development of Applications for the Internet of Things. For this purpose, COMPOSE takes a similar approach as ICORE and abstract from physical things and models them as virtual entities, so called service objects. They are simple units which can generate data for further processing and can be composed into units performing more complex data processing task.v] RERUM: The main objective of RERUM is to develop, evaluate, and trial an architectural framework for dependable, reliable, and secure networks of heterogeneous smart objects supporting innovative

Smart City applications. The framework will be based on the concept of "security and privacy by design", addressing the most critical factors for the success of Smart City applications.

5) OpenIoT: OpenIoT is an open source middleware for getting information from Internet connected devices, sensor networks, or simply sensors connected to the Internet and allows you for deploying and executing new intelligent services without worrying what exact "things" are used for provisioning the services. The open source OpenIoT project is offered as implemented reference framework enabling a new range of largescale intelligent and dynamically defined Internet of Things applications, by following cloud computing delivery models.
6) IoT6:- IoT6's main concerns are with how IPv6 can contribute to IOT aspects of governance, security and privacy. The main focus is on studying applications in smart buildings – mainly using legacy equipment. In Table.1 let us have a look at technical solutions from the FP7 projects, which mainly compose of the AC05 cluster.

TABLE 1

Privacy protocols of IOT implemented in different projects of FP7 [4].

PROJECTS	**PRIVACY**
1] ICORE	Usage control tool-kit.
2] BUTLER	Privacy solutions.
3] GAMBAS	Anonymous data discovery.
4] RERUM	Privacy enhancing technology (PET) for adequate protection of citizen's privacy in smart city application.
5] COMPOSE	Usage control, sticky policies, static analysis, declassification, data provenance and Security contracts.
6] OpenIoT	Implemented role based assignation algorithm.
7] IoT6	Mapping of device properties to IPv6 network address through identifiers, which are stored in protected areas.

C] REQUIRED CHARACTERISTICS IN IOT:-

Performance checks of the privacy impact assessment prior to the launch of a new IOT service must be done from different angles. Privacy by design and privacy by default principles should be applied. It will be easy to setup a better privacy if interlinked devices support common protocol and works on standard platforms. Each device should be capable enough to segregate different user thus managing confidentiality and privacy of different users. Fig 6 tells about characteristics of IOT privacy [8]. More robust protocols need to be implemented in the middleware for better privacy policies management. Openness, transparency and purpose specification while collecting data. Inability to track users based on identity by hiding geo-location [8]. User query privacy needs to be provided. Limitations on personal data collection need to be implemented [8]. New trends need to be introduced in IOT apart from user-centric to contextcentric and self-adaptive privacy preserving mechanism and protocols need to be developed.

We must balance a combination of technical and legal means to achieve privacy enhancing solutions in IOT.

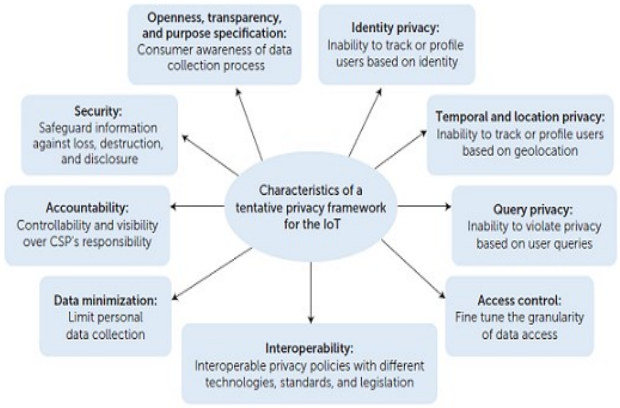

Fig 6: Characteristics to include when developing an IOT privacy framework [4].

6 PHYSICALLAYERSECURITY METHODS

Need for Physical Layer Security models: Communication security plays a very important role in overall security semantics of Internet of things due to their wide application area such as commercial, industrial, government, and military application. Internet of things utilizes air as medium of communication implementing various radio-access technologies like Bluetooth, NFC, GSM, IEEE 802.15.4, etc. Also in future, device communication with use of VLC, acoustic and molecular technologies is possible [6]. Traditional Cryptographic algorithms can't be applied directly as these algorithms require large computation power and energy resources where no of MTC connected devices are large along with their heterogeneity. To overcome this issues, physical layer security methods are used that can provide unbreakable or perfect secrecy by exploiting channel's characteristics. We will review few methods that successfully address to IOT application device requirements such as limited hardware and computing power, low data rate requirements, limited storage requirements and complex form factors [6].

Censoring: This technique is based on distributed binary detection problems where sensors implement appropriate countermeasures to make eavesdroppers acquired data useless to recognize sensors appropriate state. Censoring techniques makes use of Ali-Silvey distances to characterize detection performance under physical layer security. This transmission scheme effectively addresses energy constraints while giving a perfect secrecy. However, this model works on perfect knowledge scheme where

eavesdropper or intruder knows the network is energy constraints and implements its best strategies while networks also knows the potential computation and operational capabilities of eavesdropper. Intruder is also less informed than the legitimate receiver by presence of a degraded channel where intruder can only detect whether sensor transmissions are present or not. Following Fig 7 from Marano et al explains the abstract working model of censoring technique [13]. This technique uses 2 divergent threshold function pairs where one of them is strictly decreasing while another is strictly increasing function from certain constraint. This is used for calculation of likelihood ratio which can be used as a metric for probability that eavesdropper detects true hypothesis. Sensor only sends its data when its likelihood ratio is either very high or very low while others stay silent thereby preserving energy [6].

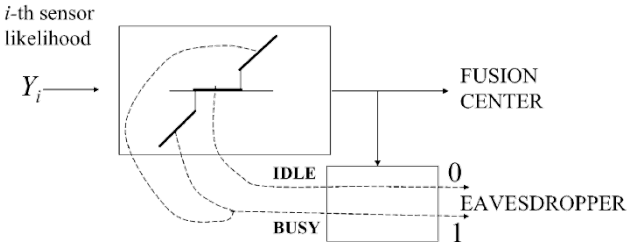

Fig 7: Working of Censoring Technique where eavesdropper gets degraded channel which only can infer whether channel is busy or not [13].

Channel Aware Encryption: This technique is modification of channel based flipping scheme where each sensor can take 3 actions which either they are in sleep or they are reporting non-flipped decision or they report flipped decision. Flipping a decision involves inversion of quantized bits of data i.e. 0 changes to 1 and vice-versa. Fig 7 from Jeon et al and Choi et al. explains general idea behind channel aware encryption where the main and eavesdropping channels are represented as solid and dotted lines, respectively [14]. The received signals at the AFC and EFC are corrupted by Gaussian noises respectively [14]. AFC first broadcasts the 4 thresholds T1 to T4 which are strict decreasing order i.e. T1>T2>T3>T4 along with pilot signals which makes sensors acquire channel state information. However both AFC as well as EFC doesn't know main channel gains of a corresponding sensor to AFC.

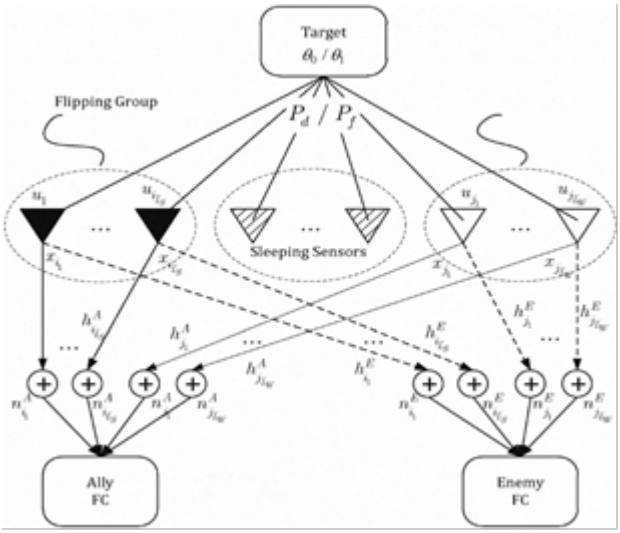

Fig 8: Flipping and non-flipping groups intermixing to confuse and randomize channel to Enemy FC Channel Aware Encryption Technique [14].

Based on this main channel gains and thresholds T1 to T4 it decides whether to encrypt data i.e. to flip their decision or send unaltered data or remain dormant. EFC is unable to identify which sensors have flipped their data since it doesn't know channel fading gains since EFC channel is independent of main channel and doesn't have statistical dependence. This is known to an AFC which on receiving discards the flipped decisions to obtain data securely and eventually leading to perfect secrecy [14].

Summary of Channel Aware Encryption and Censoring Techniques:

1] Channel Aware Encryption has minimum CSI encryption and minimum computation complexity while censoring has minimum CSI requirements.

2] CAE and Censoring platform well on Energy constraints with use of simple computation.

3] Both CAE and Censoring platform well on scalability i.e. stability exists with no increase in connected devices.

4] CAE and Censoring techniques lead to perfect or unbreakable secrecy.

However for futuristic Internet of Things operations where no of eavesdroppers is not limited or their information is unavailable to AFCs, we need a solid well founded holistic framework that take into consideration all the requirements of physical layer security. Also since both above mentioned techniques are yet to experimented on a potential very large network, it is not possible to decide one of framework or model as solution to Internet of Things based alone on simulations of these algorithms. Also with applications of new technologies like VLC, molecular communications apart from AFC in communication, we need an abundant research in current technologies.

7 COMMUNICATION TECHNOLOGIES FOR INTERNET OF THINGS

Trusted interaction across devices and networks in IOT architecture which has devices and systems connected via heterogeneous network employing various standard protocols. They enable powerful services but also expose systems to various risks eavesdropping on message, DOS, DDOS and message falsification. To protect against these potential threats, IOT devices and systems require secured communication capabilities. However IOT business opportunities rest precariously on one critical factor – Communication security. A series of recent hacks has revealed the communication security gap. As per [24], in 2014 an Israeli security firm found out vulnerability in telematics device developed by Zubie, a US based connected car startup. They found out that zubie hardware which provided drivers instructions on improving driving efficiency did not encrypt information properly and how hackers could send malicious updates to device, get cars location and even unlock doors remotely [24]. Thus a secured communication is must in IOT. Let us study of IOT protocols on top of existing architecture model like OSI model for proper communication. In table 2 we have broken protocols into layers for proper organization.

TABLE 2
Layers and protocols in IOT architecture

Layer	Protocol
1] Infrastructure	6LOW PAN, IPv6, RRL
2] Identification	EPC, u-code, URIs
3] Transport	Wi-Fi, Bluetooth, LPWAN
4] Discovery	Physical Web, DNS-SD
5] Data	MQTT, COAP, Node
6]Device Management	TR-069, DMA-DM
7] Semantic	JSON-LD, Web thing model
8]Multi-Layer Frameworks	Alljoyn, IoTivity, Weave, Home Kit

IOT Communication can be secured by following rules:1] Identify and document threats, Apply popular STRIDE model (Spoofing identity, Tampering with data, Repudiation, Information Disclosure, Denial of service, Elevation of Privilege)[25].

2] A set of Data Link and Transport protocols implemented. Each protocol support varying level of security for better confidentiality and authentication [25].

3] Securing supply chain by securing hardware, firmware, OS, protocols, cloud providers. This can be achieved by integrating third party applications to avoid any vulnerability while adapting to updated version of other interrelated product. Ideally, maintaining license agreement with IOT device vendors [25].

4] Exercise network access control (NAC) to unify endpoint security. Gateway should allow access to only selected secured documented MAC address [25].

5] Using Multiple Service set Identifiers (SSID) in wireless network and Private Pre-Shared Key (PPSK) to ensure each sensor connects securely.

6] Using Anti-jamming devices to avoid hackers from conducting DDOS attack or Radio signal attack on sensitive sensors for example medical devices like pace makers been hacked and drained of battery power [25].

8 DATA SECURITY

Given the potential volume of Machine to Machine traffic, internal storage system will struggle to scale in cost effective manner, along with reducing size of chipset. Thus most data is going to be cloud based. With an expected hit of 30-50 billion devices by 2020 there will be huge security concerns to mitigate each security glitch. From Fig 9 it is clear that how Data Security and Privacy are most important and critical factor to be considered [3]. When multiple organizations share resources there is risk of data misuse. So, to avoid risk it is necessary to secure data repositories and also the data that involves storage, transit or process. It needs to address 4 main characteristics i.e. huge volume i.e. BIG data coming from large number of sources in different versions and formats with 3 triads of security i.e. Confidentiality, Integrity and Availability which are addressed as follows [10].

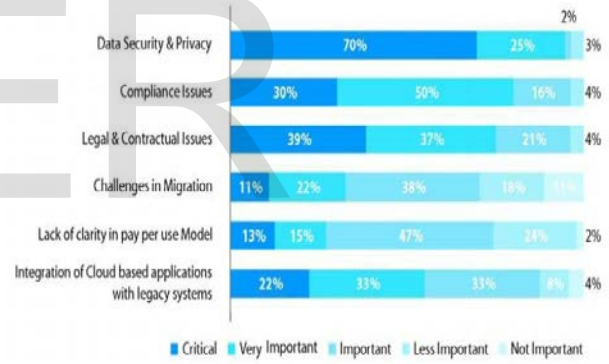

Fig 9: Data Security and Privacy importance [3].

Data Confidentiality: Access Control and encryption are 2 major techniques that preserve data confidentiality. Automatic authentication with authorization will be requirement of IOT data as human intervention in every data access is not possible. This automatic authentication should integrate large number of different access control mechanisms effectively considering their heterogeneity along with maintaining speed of data access for IOT.

Data Privacy: Achieving data privacy is highly complex since it depends on many factors like data sharing and data acquisition policy, allowing user data for its personal use and public use differently and so on. Mechanisms which check user's personal data usages are adhering to privacy implications of user must be developed.

Achieving ease of data on request along with strong privacy and confidentiality is always a tradeoff. Let us have a look at data security risks and solutions on it for IOT devices

transmitting data continuously to and fro on open unsecured network [11].

a. Symmetric Encryption techniques like Advanced Encryption Standard (AES) which has comparatively less overhead than asymmetric encryption techniques. Thus saving on memory, computational costs and utilizing node energy efficiently. However it has few risks associated with it like an insider attack which may put several computers on risk due to symmetric key encryption. Device certificates for strong authentication in communication by encrypting data transmitted through IOT systems via network thus protecting against popular cryptanalytic attacks such as BruteForce attacks.

b. To minimize the number of transmissions in sensor network a hybrid method of compressive sensing (CS) is used. Data secured by using Advance Secured and Efficient Transmission-Identity SET-IBS protocol used. To provide security the Advance-Secured and Efficient Transmission-Identity Based Digital Signature (Advance-SET-IBS) is used to encrypt the sensed data.

On each sensor node the Encryption Algorithm Advance SETIBS is implemented to secure the data. An Advance IBS scheme implemented for CWSNs consists offollowing four operations that are First setup at the BS, Second keyextraction, and third offline signing at the CHs, Fourth online signing at thedata sending nodes and Fifth verification at the receiving nodes. Let us have a look at the comparison table which clearly shows benefits of SET-IBS/SET-IBOOSover other protocols. Regular updates and patches are dispatched and automatically updated so that system stays up to date. For example: small connected sensors need to be updated with latest software patch and updates against latest threats and encryption techniques for enhanced performance and security.

Thus our final word in sensor data security is to keep innovating IOT for a better and secure future. Further we can implement Lightweight Enhanced lossless Entropy Compression (LEC) algorithm for better efficiency. More complex cypher like ECC needs to be implemented which provides more advanced security without any tradeoff in computational cost. Data Confidentiality needs more research including a better policy for access control and encryption. Major issue of Big Data is data privacy which needs relevant research. The area of encryption techniques is an active and important research area. However strong security cannot be achieved by devising new cryptographic protocols but by implementing it correctly which still remains a hot research topic. Protecting Applications is crucial for data security as attack to steal data often use applications vulnerabilities. So even though we have several techniques such techniques need substantial extension to fit IOT devices.

TABLE 3

Comparison of Characteristics of the proposed protocol with other secure data transmission protocols

	SET-IBS/SET-IBOOS	Prior Protocols
Key Management	Asymmetric	symmetric
Neighborhood authentication	Yes	Limited
Storage Cost	Comparatively low	Comparatively high
Network Scalability	Comparatively high	Comparatively low
Communication overhead	Deterministic	Probabilistic
Computational overhead	Comparatively high	Low-high
Attack resilience	Passive and active attacks on wireless channels	

9 UNEXPLORED ISSUES IN CLOUD COMPUTING

Need for focus on cloud security perspective to Internet of Things:

As Internet of things will involve billions of devices, it will lead to production of big data, we need a platform that can successfully provide storage, remote processing power and analytics of data to improve service quality and human lives better. As a result cloud and internet of things are inseparable. Although cloud is backbone of Internet of Things architecture, it is not getting the required attention as sensor and device security is taken into consideration in terms of research and better solutions. Attacker could exploit several less secured vulnerabilities to gain an entry into secured network. As Singh pointed out 20 considerations in context of cloud security with respect to internet of things, we notice only those considerations in cloud security where substantial research is needed [9].

Data Combination: Although use of data analytics is imperative in internet of things to give a better service, proper techniques and algorithms must be developed so that identification of unique entity is impossible through use of data aggregation. In study of A Narayan it is found that information which can be used for distinguishing a person from another can be used on aggregated data to recover complete information about a particular person [20]. Differential privacy which works on addition of mathematical noise such that individual privacy gets protected can be one of the solutions [15] [16]. However more research needs to be done to counter attacks on differential privacy such as timing attacks, state attacks and privacy budget attacks [2]. Homomorphic encryption which enables simple data operations on encrypted data can be one of futuristic solutions to cloud computing [17]. Architectures which can support multiplication of large numbers using full Homomorphic encryption have been proposed, it is still in beginning stage where it is incapable of handling big data. Last but not least, privacy of user data depends on trustworthiness of cloud service provider which in turn addresses not to pure technical solutions but also social-economic reasons [9].

Auditing framework: SLAs are established when contracts is being made by a cloud service provider. SLAs denotes the ways in which service will be delivered and various terms and conditions on resources provided by cloud

tenants. However, there is a need for 3rd party which checks whether consumer receives the service for which they pay and also addresses various security problems during service functionality. Auditing framework provides data which can be used for finding out false data leakage, enforcements of government policies and compliance with SLAs. Only few architectures have been developed that perform dynamic auditing but all are based on lightweight devices [26]. Due to billions of devices in internet of things, automatic audit generation is still a topic that needs exceptional research. Also in future there is need for change in policies of tenants so that negotiating terms and conditions are possible.

Transparencies between Cross layer data sharing policies: As we know, cloud tenants can provide 3 types of services i.e. IaaS, PaaS, SaaS they might use various 3rd party services for other technical needs like one tenant might use another IaaS provider for complete PaaS service. However, it is important to bring more transparencies within various data policies provided applied to 3rd party services by cloud tenants. Also as indicated by Singh [9], application level composition might lead to several vulnerabilities. Although Henze et al presented with cross layer data annotations, it is imperative to design new framework that will take into consideration all complexity of internet of things and big data, so that user privacy is protected [18].

Effects of decentralization of cloud services on internet of things: Decentralizations of cloud gives rises to both positive effects and negative effects. Decentralized cloud might be prevented from global denial of service attack but on failure it might lead to identification of unique users.

Decentralization leads to overall increase in functionality, scalability but it also leads to lack of global authentication and possibility of more data leakages due to more data transfer. Also overall managements of fragmented parts are difficult compared to management of whole unit. Also as per *Renuka Prasad Pasupulati*, decentralized nature prefers flexibility, it also adds burden of extra computations [19]. As a result, more stronger and concrete decentralized frameworks are needed in internet of things where interactions are complex and dynamic.

10 Conclusion

In this paper, we tried to simplify IOT security by breaking it into major paradigms and tried to represent ongoing state of IOT security. We described possible threats and attacks on Internet of Things, emerging architecture which provided with 4 major features which are absolute necessity in realistic IOT architecture. Also, communication technologies and physical layer security methods for securing entire transmission of data were also depicted. Thus we have studied how data is likely to be tempered in IOT devices, how securing all data is not important as only few data can be marked as one with high priority and more encryption can be given to it compared to rest data that sensor keeps collecting. Thus saving time and computation speed along with maintaining CIA (confidentiality, Integrity and availability) principles. Survey on depicting a need for more robust privacy policies implemented in IOT devices thus giving end user a more sense of safety. We also outlined unexplored areas in cloud security where more research work needs to be done.

11 References

[1] Fei Hu, Security and Privacy in Internet of Things (IoTs) Models, Algorithms, and Implementations, pg 46-461, 2016.

[2] Jessye Dos Santos, Christine Hennebert, Cýdric Lauradoux, Dec. 2015, “Preserving privacy in secured ZigBee wireless sensor networks”, IEEE.

[3] R. Velumadhava Rao, K. Selvamani, “Data Security Challenges and Its solutions in Cloud Computing”, ICCC, 2015.

[4] Ted Levitt, January, 2015, “Internet of Things”, ERCIT.

[5] Smart Light bulb Hack Lets Others Steal Your Wi-Fi Password http://www.trendmicro.com/vinfo/us/security/news/internet-ofthings/smart-lightbulb-hack-lets-others-steal-your-wi-fi-password

[6] Amitav Mukherjee, “Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints”, IEEE, October 2015.

[7] Madhumita Panda, “Data Security in Wireless Sensor Networks via AES Algorithm”, ISCO, 2015.

[8] Pawani Porambage and Mika Ylianttila, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, Athanasios V. Vasilakos, “The Quest for Privacy in the Internet of Things”, IEEE 2016.

[9] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers, “Twenty security considerations for cloud-supported Internet of Things”, IEEE, 2015.

[10] Elisa Bertino, 2016, “Data Security and Privacy in the IoT”, IEEE.

[11] ELISA Bertino,”Data Security and Privacy Concepts, Approaches, and Research Directions”, IEEE, 2016.

[12] Gianmarco Baldini,”IoT Governance, Privacy and Security Issues”, European Research Cluster on Internet of things, 2016.

[13] Stefano Marano, Vincenzo Matta, and Peter K. Willett,”Distributed Detection With Censoring Sensors Under Physical Layer Secrecy”, IEEE, 2009.

[14] Hyoungsuk Jeon, Jinho Choit, Steven w. McLaughlin and Jeongseok Ha ,”Channel Aware Encryption and Decision Fusion for Wireless Sensor Networks”, IEEE,2011.

[15] Xiaoming Yao, Xiaoyi Zhou, Jixin Ma, “Differential Privacy of Big Data: An Overview”, IEEE, 2016.

[16] Chien-Lun Chen, Ranjan Pal, Leana Golubchik,”Oblivious Mechanisms in Differential Privacy Experiments, Conjectures, and Open Questions”, IEEE, 2016.

[17] Kamal Kumar Chauhan, Amit K.S. Sanger, Ajai Verma,2015 ”Homomorphic Encryption for Data Security in Cloud Computing”, IEEE.

[18] Martin Henze, Rene Hummen, Klaus Wehrle,”The Cloud Needs Cross-Layer Data Handling Annotations”, IEEE, 2013.

[19] RenukaPrasadPasupulati, Jordan Shropshire,”Analysis of Centralized and Decentralized Cloud Architectures”, IEEE, 2016.

[20] Andreas Haeberlen, Benjamin C. Pierce, Arjun Narayan," Differential Privacy Under Fire", IEEE, 2011.

[21] A. Narayanan and V. Shmatikov, "Myths and fallacies of personally identifiable information," Comm. ACM, 2010.

[22] Design-Spark "11 IOT Protocols you need to know", http://www.rsonline.com/designspark/electronics/knowledgeitem/eleven-internet-of-things-iot-protocols-you-need-to-knowabout.

[23] "IOT standards and protocols", Postscapes, http://www.postscapes.com/internet-of-things-protocols

[24] Capgemini Consulting "Securing the Internet of Things Opportunity: Putting Cyber-security at the Heart of the IOT", 2014.

[25] Cloud Security Alliance, "Security Guidance for Early Adopters of the Internet of Things (IoT)", 2014

[26] Lo-Yao Yeh, Pei-Yu Chiang, Yi-Lang Tsai, and Jiun-Long Huang,2015,"Cloud-based Fine-grained Health Information Access Control Framework for Lightweight IoT Devices with Dynamic Auditing and Attribute Revocation", IEEE.