International Journal of Informatics and Computation (IJICOM)
Vol. 1, No.2, December, 2019
ISSN: 2685-8711, E-ISSN: 2714-5263

A Survey of Network and Information Security

Wanda P[1], Jin J. H.[2]

Abstract
Security threats and shows abnormality about security, safety, privacy and trust as network security-related data, in short, security-related data. Apparently, the first step to detect network attacks and intrusions is to collect the security-related data. In this paper, we will present a lot of approaches to solving Networks and Information Security issues. We survey network security in LTE technologies, Vehicular Ad-Hoc Network, and security in Wireless Sensor Network. Internet of Things. In this paper, we describe many methods in Information Security. Is consist of Information Security in Big Data and Cloud Computing.

Keywords
Survey, Network, Information Security

1. Introduction

Security threats and economic loss caused by network attacks, intrusions, and vulnerabilities have motivated intensive studies on network security. Typically, data collected in a network system can be used to detect security threats. We define these data as network security-related data. Studying and analyzing security-related data can help detect network attacks and intrusions, thus making it possible to measure the security level of the whole network system further. The first step in detecting network attacks and intrusions is to collect security-related data.

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals.

Corresponding Author: Wanda P(wpwawan17@yahoo.com)
1 Wanda P, University of Respati Yogyakarta,
2 Jin. J.H, HUST, China

Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

With the rapid development of network and communication technologies, there has been increasing amount of attention on the security of network systems [1]. Network security is usually reflected by relevant data generated, originated or extracted from the network system. By studying the data related to network security events, the security of the network system can be quantified and measured.

Security threats and shows abnormality about security, safety, privacy and trust as network security-related data, in short, security-related data. The first step to detect network attacks and intrusions is to collect the security-related data. Generally, network data can be collected from both the output and input of a system and plays a vital role in IT as it is crucial in managing and troubleshooting network system, detecting network intrusions, and billing network traffic

Usually, data anomalies can reflect network attacks and intrusions. Thus, we can detect network attacks by searching for abnormal network data. We refer this kind of data that can help reflect the security status of a network system as network security-related data, and they may be feature, signature or fingerprint of a specific attack behavior [2]. For example, Time To Live (TTL) is a type of network security-related data. TTL specifies the maximum number of segments allowed to pass before a router discards an IP packet.

.

2. Network Security Survey

2.1 Network Security in LTE Technologies

The long-term evolution (LTE)/LTE-advanced (LTE-A) network provides advanced services for billions of users with its higher bandwidths, better spectrum efficiency, and lower latency than legacy cellular networks. However, it still suffers from new security threats due to its all IP-based heterogeneous architecture. Therefore, there is a critical need to perform rapid and accurate network security measures in the LTE/LTE-A network. To achieve LTE/LTE-A network security measurement, security-relevant data (in short security data) collection and data analysis for attack detection are required as prerequisites.

In recent years, the jamming detection methods in wireless sensor networks and ad-hoc networks have been widely researched. However, there is little available literature related to detecting LTE/LTE-A jamming attacks, and in most cases, this kind of attacks are difcult to detect and resolve. Xu et al. [3] discussed the effectiveness of three single measurements as the basis for detecting a jamming attack, including signal strength, carrier sensing time, and Packet Delivery Ratio (PDR). The results showed that no single measurement is sufficient to determine the presence of a jammer under certain circumstances. Both signal strength and carrier sensing time can only detect the constant jammer and deceptive jammer, but they are powerless in detecting a random jammer or a reactive jammer.

Fragkiadakis et al. [4] presented an anomaly-based intrusion detection algorithms by observing the changes in the SNR statistical characteristics including average SNR, minimum SNR, and max-minus-min SNR. The authors first investigated local algorithms using simple threshold algorithms and Cumulative Sum (CUSUM) algorithms respectively;

then they investigated a fusion algorithm using Dempster-Shafer algorithm to fuse the output of the local algorithms and collaboratively detect jamming attacks.

Lichtman et al. [5] proposed a jamming detection method for LTE/LTE-A especially on the PUCCH based on monitoring the excess PUCCH energy and an abnormal amount of PUCCH errors. The power levels on the PUCCH should be by the transmit power commands assigned by e-NodeB, so the detection method uses a simple energy detector on the baseband samples to detect the presence of excess energy or abnormally high amount of energy in the PUCCH region. The detection method based on the abnormal amount of errors monitors the bit errors in received Channel Quality Indicator values to seek for the sudden increase in errors on the PUCCH and compares to other physical channels like PUSCH to determine if there is a jamming attack.

The LTE/LTE-A signaling attackers always send malicious wake-up packets to trigger the bearer setup procedure, this can lead to transmission of a large number of control messages among different network elements and saturate the LTE/LTEA network's resources, so most of the signaling attack detection methods are based on the observation of bear inter-setup time or the wake-up packet generation rate [6].

Bassil et al. [7] proposed a detecting method for signaling attacks. The collected data used for detection include UE number, bearer number, and time of activation or deactivation of a particular bearer. The number of bearer requests per UE and the inter-setup time can be obtained from the above data. The resulted in obtaining the average lifetime per bearer, and the number of bearer activation requests issued by a specific UE for a specific bearer.

Gupta et al. [8] collected features of uplink wake-up packets, like their frequency, destination IP, destination port, etc. to obtain a set of feature vectors, containing normalized destination IP entropy, normalized destination port entropy, normalized source port entropy, normalized packet length entropy, normalized wake-up rate, variance of inter wakeup times, response-request ratio. Support Vector Machine (SVM) was used to perform supervised learning of standard data. This work needs to calculate a set of vectors in data collection procedure so that the efficiency may be not good. Privacy and resource consumption were not considered in this work.

Pavloski et al. [9] proposed a simple signaling attack detection mechanism by observing the fact that their low band-usage of communication resources can identify this kind of attacks. The data containing the total connected time and the connection but no data transmission time can be collected in each mobile device or in a centralized node such as eNodeB for detecting this attack. The proposed method defines a cost function using Exponential Weighted Moving Average (EWMA) and decides by comparing a real-time cost with an average cost in a period.

Then we will review some detection methods that focus on SIP message attacks and SIP flooding attacks. The following presents the detecting methods against abnormal SIP messages. Wahl et al. [10] presented a signature-based anomaly detection method in which SIP messages are embedded in a vector space to reflect the characteristics of the SIP traffic. The presented method first extracts feature strings using the definitions of ``tokens'' and ``n-grams'', then both global and local anomaly detection methods based on geometric learning models are used to detect unknown attacks. The core of geometric models is to calculate the Euclidean distance in the vector space.

Nassar et al. [11] presented an online monitoring approach based on SVM to detect SIP-related attacks. In the proposal, the SIP traffic is cut into small slices, and 38 features of

SIP traffic flows are extracted containing general statistics, Call-ID based statistics, distribution of final state of dialogs, distribution of SIP requests, and distribution of SIP responses. These features are the input of an SVM learning machine. This method performs well for detecting flooding attacks and Spam over Instant Messaging (SPIM)

Given that the malformed SIP messages attacks and the SIP flooding attacks are the most common attacks on IMS, we here list some detection methods that specifically target at these two attacks. Seo et al. [12] presented an anomaly detection method based on Stateful Rule Tree. The main idea is refining the rules of original RFC 3261 rules and creating a rule tree structure. In the detection of malformed SIP messages, they applied a rule matching algorithm to check if the header of a packet follows the security rules they designed and detect unmatched or undefined message headers. In the detection of the SIP flooding attack, they adopted the state transition models in the RFC 3261.

Zhang et al. [13] presented an automatic detection scheme of SIP flooding attacks and SIP malformed messages attacks on VoLTE. To detect the former attacks, it employs threshold-based algorithms in which the instant amount of SIP packets received from VoLTE interface within one minute is compared with a threshold. Nevertheless, determination of the threshold is not specified, and experiments did not evaluate the performance of their detection scheme.

The detection methods for SIP flooding attacks have drawn many researchers' attention. Introduced below are some work concern with SIP flooding attacks. Lee et al. [14] presented a statistical and learning-based detection method for SIP flooding based DoS attacks. The presented algorithm compares merely the collected factors of the traffic including IP, URI (Uniform Resource Identifier), Call-ID, and Method (e.g., INVITE, BYE) with their detection rules. Every detection rule has a corresponding threshold value that is updated dynamically.

Zhang et al. [15] presented an SMS spammer detection scheme based on behavior analysis. The scheme integrates multiple behavior attributes of users and extracts statistical properties from SMS records which record the information of each SMS, including calling number, called number, transmission time, receiving time and message length. Then five machine learning algorithms including Binary Decision Tree, Random Forest, SVM, Logistic Regression, and SelfOrganized Feature Mapping are used to train the classifier of spammer and non-spammer.

The content-based SMS spam detection techniques may touch upon user privacy issue and huge memory requirements at the server side. The latter detection system in the network side can help to reduce the cellular bandwidth consumed by SMS spam and achieve real-time transmission of the massive SMS messages. The detection can be based on behavior analysis, content-based analysis, subscriber feedback-based methods, sender reputation-based schemes, and traffic analysis technologies [16][17].

2.2 Network Security in Vehicular Ad-Hoc Network

The vehicular ad-hoc network is an emerging area of networking. It is a subset of Mobile ad-hoc networks. The vehicular ad-hoc network that provides Vehicles to Vehicles (V2V), Rode-side Unit to Rode-side Unit(R2R) and Vehicles to rode-site Unit (V2R) communication[30]. In recent years, more accident cases are found significantly. Due to this, roads are found to be more congested and busy. With the help of dedicated short-range communication (DSRC), VANETs establishes communication between various vehicles which are changing their direction frequently. Vehicles directly communicate with different vehicles and send information regarding traffic jams, warning messages with the

road-side unit (RSU) which is fixed equipment in roads.

Vehicles communicate with another vehicle directly if there is wireless connection available; it is called single hop vehicle to vehicle (V2V) communication. If there is lack of direct connection between them then, forward data from one vehicle to other vehicles until it reaches proper destination its called multi-hop vehicle to vehicle (V2V) communication.
The Security is more crucial in VANETs due to lack of centralization, dynamic topology. Due to this, it is difficult to identify malicious, misbehaving and faulty nodes or cars in the network. Mainly trust models are based on verifying vehicles and provide appropriate trust value to all vehicles. Trust should be provided either directly or indirectly

Hong x. Et al. [18], proposed establishing trust management scheme with three aspects, which are policy control, proactive trust establishment, social network impact on the network. Policy control considers entry trust and data trust attributes are used. Proactive trust considers traditional approach according to past communication history of that car/node for the trust value. Social trust considers nearest vehicles opinion and setting up trust in another vehicle.

Jorge h. Et al. [19], proposed watchdog algorithm with intrusion detection techniques for establishing trust management. In that source node sent packets to the neighbor node and monitors that node with ids. It is forward that packets than maintain its trust value in trust table otherwise that decrease trust value of that node. The drawback of this technique is to create collision in the network, and monitor that node until that forward or drop. It has contained huge monitoring history of the neighbor node if it has a large number of neighbor nodes. Cong l. Et al. [20], proposed trustworthiness based on incident reports in V2V communication and forward to those vehicles. Crowdsourcing capabilities use for evaluating trustworthiness value for vehicles. The global view can broadcast for individual vehicles trust value in CSC. Future work includes security and privacy issues using unique identification and public key infrastructure mechanism.

Zhou w. Et al. [21], proposed to establish Dynamic trust token based on the method used for co-operation with nodes. Both cryptography mechanism should be included for packet integrity with the symmetric and asymmetric algorithm and applies neighborhood watchdog algorithm which generates tokens for checking packet is either valid or not. In this algorithm protection of packets during communication is increased and latency of network is decreased. It is cooperative packet forwarding schemes applying for communication. It is set up for instant trust at runtime communication. The drawback of this technique is not encouraging misbehaving node to well-behaving, don't punish malicious node and not reward right nodes.

Subir b. Et al. [22], proposed id-based techniques used for verification of cars with the public key without a certificate. The proxy server provides message authentication and trust management. Safety message delivered through RSU (rode site unit) and id-based signature properties imply on the proxy signature with ECDSA. In this technique authentication and trust, management is dynamic and untrustworthiness. RSU which had proxy signature pre-stored handles trust management scheme.

Tahani g. Et al. [23], proposed Markov chain model for establishing trust management. This model not only considers the behavior of a node in dynamic trust metric but that monitor all constraints activity of that node. Each vehicle treated as monitoring an updating trust metric table of its neighbor nodes belong to that behavior. Misbehaving and selfish vehicles identified with this mechanism. It uses time interval and number of transition with other nodes in trust management. This system uses stress and trust evolution system for trust

model. In this global trust should not be established which is the future scope of this mechanism. Yu-Chih w. Et al. [24], proposed road site unit (RSU) and beacon based trust management system to improve safety and location privacy. This techniques motto is quick message opinion and prevents sending and forwarding from the internal malicious node. This technique takes a decision quickly and provides an opinion in less time Drawback of this mechanism is not able to compare trust value with another node.

Felix g. Et al. [25], proposed to provide trust based on TRIP (Trust and Reputation infrastructure based proposal) algorithm for traffic analyzing. TRIP identify malicious and selfish node which spreading bogus or false information in the network. Message and traffic warning message sent to another node that checks the reputation and accurate value of that node. If the node is malicious than reject and drop packets from those nodes/cars. Fuzzy logic classifies and categorizes trust value as per operation and advertisement messages. The reputation score is computed with three information's: previous experience, surrounding vehicles, and recommendation of the central authority. Three types of trust values: Not trust-reject all packets, +/- trust-accept but not forward and trusted- accept and forward. The drawback of this mechanism is hard to maintain trust value and behavior of the node, and we cannot identify the node is honest or malicious

Tahani g. Et al. [26], proposed trust model depends on public key infrastructure for trust management and distributed cluster algorithm. VANET dynamic demilitarized zone, its set of vehicles of neighbors provide confident, and there is registration authority (RA) provide authentication to each vehicle within particular cluster head (CH). This technique prevents malicious and unknown vehicles which are authenticated within the cluster. Cluster head defines as trust level and vehicles CA. Cluster algorithm is based on two parameters: trust metric used for define trust level of vehicles and mobility metric.

Qing d. Et al. [27], proposed event-based reputation model for filtering bogus messages. Role-based reputation mechanism is used to determine the incoming message is significant and trustworthy to the drivers/cars. It enhances trust for the vehicular network. This technique includes random waypoint which is not sufficient technique for reputation. In future, we can imply fuzzy logic for calculating reputation value for an event.

Tahani g. Et al. [28], proposed hybrid trust model for determines trust metric. Two terms used for monitoring trust: cooperation with other vehicles in network and broadcast legitimate data. The fuzzy based algorithm used to decide the honesty of vehicles and filter out malicious vehicles. One trusted neighbor to issue CA in the PKI is distributed among some vehicles. Trustworthy value is calculated through monitoring cooperativeness of monitor vehicles and forward calculated trust to neighbor vehicles. Yi-Ming c. Et al. [29], proposed Beacon-based trust management (BTM) techniques prevent the internal attackers from sending false or bogus messages in privacy enhancement in the network. Secure beacon based trust protocol is used to evaluate direct and indirect trust management scheme. Direct trust in trustworthiness value and indirect trust opinion transmitted from multiple vehicles. Dempster Shafer evidence theory is used for numerical computation.

Chen c. Et al. [30], proposed data aggregation mechanism to establishes trust in the network. it is used to check the quality of the message. This method uses multiple existing identities based aggregation methods like concatenate signature base, onion signature base, and hybrid signature base combines into one aggregate signature summing them mathematically. It eliminates signature redundancy of aggregation signature, flexibility to aggregation function no harmful effects in the network. The drawback of this algorithm is signature size is much higher and no comparative mechanism.

Rashmi s. et al. [31], the proposed trust-based approach in clustering and ant colony routing, clustering techniques create a cluster and consider the position, direction and speed of relative vehicles manage networks/cars. Cluster head (CH) considering real-time update location and trust value of that vehicles. Direct and Indirect trust mechanism used to establish the trust. Trust management used to find out the most trusted path between two nodes of a VANET.

2.3 Network Security in Wireless Sensor Network

The Wireless Network is the network in which the communication between the sender and receiver host is possible without any cable connection. The wireless network is advanced to a wireless network because it reduced the cost of the extra link is connected to the particular host in the network. The different devices in the wireless network are performing their role efficiently to maintain the reliable connection in between source to destination

Wireless sensing element network is more vulnerable as compare to wired or wireless communication however in currently, number of analysis focus within the field of WSN, therefore in future the WSN is a most utilized network in a real application in every were. In this section, we have a tendency to study a range of latest papers beneath security and energy connected issue and its resolution in WSN field those are as follows.

In this paper [32], we aim to provide a mechanism which is used to detect the vampire attack in WSN. Vampire attacks can be defined as the transmission and composite on of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination. We discuss the effect of vampire attacks on Ad-hoc On Demand Vector Routing (AODV). AODV is a reactive protocol which maintains routes only between nodes which need to communicate. The routing messages do not contain information about the entire route path, but only about the source and destination.

In this paper [33], a novel trust routing scheme is proposed. Multi-agents collect multi-factors information and cooperate to decide the trust route. Trust is the degree of belief about the future behavior of other entities, which is based on the experience of the nodes. To sensor network, if WSN nodes want to communicate or exchange key data, it is necessary to establish a trust relationship between nodes to ensure the reliable data exchange. Trust is related to many factors, such as hop count node behavior node's residual energy. To enhance security and reliability in sensor network, trust routing scheme is proposed in the paper. Trust can be interpreted as belief, reputation, probability, and trustworthiness. Trust routing reflects the trustworthy degree of the routing path. In a sensor network, in addition to the traditional hop count, routing trustworthiness is related to many factors, such as node's residual energy node's attack behavior.

In this paper [34], we have analyzed a set of algorithms collectively known as CAWS and MES-1. CAWS (cellular automata based security algorithms) [35], which includes key management under cellular automata algorithm and secure data communication algorithm, which require less amount of memory and less amount of simple computation. Modern Encryption Standard (MES-1) [35], [36] is an advanced cryptography method which is used for double encryption and decryption. Modern Encryption Standard (MES-1), the method is achieved by file splitting into two parts, which is encrypted and encrypting the divided section of the file in a different form by using cipher method such as TTJSA and DJSA cipher techniques.

In this paper [37], firstly targets to evaluate these vulnerabilities to routing layer battery reduction attacks. Secondly, it focuses upon the change in an existing routing protocol to bound loss due to Vampire attacks at the time of forwarding of packets. The third aspect, this paper targets to surface outcomes measuring the functionality of various representative protocols in the existence of an original Vampire. It is the source routing, distance vector, link-state, and beacon routing protocols also a logical ID-based sensor network routing protocol have shown the effects of Vampire attacks.

In this paper [38], a continuous secure scheme is proposed for static HSN (Heterogeneous Sensor Networks) (CSS-SH). The formation of clusters in HSNs is as follows: Each L-sensor selects an H-sensor whose Hello message has the best signal strength as its cluster head. Simultaneously each L-sensor also records other H sensors from which it has received Hello messages, and these H-sensors will serve as backup cluster heads in the case that the cluster head fails. In a cluster, the cluster head can communicate with all L-sensors directly, but an L-sensor may need one or more hops to communicate with its cluster head.

In this paper [39], we consider how routing protocols, even those designed to be secure, lack protection from these attacks, which we call Vampire attacks since they drain the life from networks nodes. These attacks are distinct from previously studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but instead work overtime to entirely disable a network. Author defines a Vampire attack as the composition and transmission of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers.

In this paper [40], has represented various problems associated with security attack that coincide within the wireless sensing element network at various layers of protocol design. This paper carries with it numerous constraints in wireless sensing element network, security availability and numerous varieties of network attack and their interference mechanism at entirely different layers of the protocol stack of wireless sensing element network has been presented consecutively. This paper presents a complete introduction regarding wireless sensing element networks, sensing element network communication design and numerous application of wireless sensing element network.

In this paper [41], they propose a trust-aware distance vector routing protocol (T-AODV) to guard wireless sensing element network from wormhole attacks. Through experimental results, their proposed approach tested the network potency regarding improved packet delivery ratio, end-to-end delay, and range of node to the destination.

2.4 Network Security in the Internet of Things

Internet of Things (IoT) can be seen as a pervasive network of networks: various heterogeneous entities both physical and virtual interconnected with any other entity or entities through unique addressing schemes, interacting with each other to provide/request all kinds of services. IoT technology is expected to pave the way for groundbreaking applications in a diversity of areas such as healthcare, security and surveillance, transportation, and industry, and integrate advanced technologies of communication, networking, cloud computing, sensing, and actuation.

Given the enormous number of connected devices that are potentially vulnerable, highly significant risks emerge around the issues of security, privacy, and governance; calling into

question the whole future of IoT. IoT applications are expected to affect many aspects of people's lives, bringing about many conveniences; however, if security and privacy cannot be ensured, this can lead to some undesired consequences. This survey focuses on the security aspects of IoT and discusses current IoT security solutions.

Tahir et al. in [42] proposed a novel ICMetric based framework for securing IoT. ICMetric is based on cryptography keys. The idea behind ICMetric is a mathematical and statistical extraction of device features which, when combined, uniquely characterize the performance of a given electronic device. The ICMetric includes two stages of calculations: the calibration stage is applied only once per application domain employing some known circuits as a calibration set, while the operation stage is applied each time an encryption key is desired for a given circuit. In this paper, a solution for providing security of IoT is presented based on the ICMetric technology coupled with Secure Remote Rabbit Protocol, which secures entities and their intercommunications to provide security for IoT

Liu et al. in [43] proposed a solution for IoT security based on the principles of a biological immune system. A biological immune system has served as a role model for building IoT security. The proposed solution uses a dynamic defense frame for IoT security, since static defense strategies may prove to be inadequate. They propose a circular defense with five links: security threat detection, danger computation, security responses, security defense strategy formulation, and security defense. The links in the frame are correlated with relative data of IoT security. The behavior of a biological immune system is applied to establish links in the proposed scheme solution to make the proposed approach adaptive to the IoT environment

In [44], Zhou and Chao developed a novel architecture for media-aware traffic security and designed and evaluated the proposed security-critical traffic management scheme. The novel media-aware traffic security architecture (MTSA) meets the information security requirements for multimedia communication, computation, and service in the IoT environment. The solution is adapted to respond to the challenges and requirements of the multimedia system security in the IoT environment. It is stated that distributed privacy paradigm for MTSA, in which the authority, cost, and encryption are obtained in a decentralized manner, is a novel solution.

Lessa dos Santos et al. in [45] introduced an architecture to enable constrained devices to use Datagram Transport Layer Security (DTLS) with mutual authentication to communicate with Internet devices. This security architecture for IoT is based on a third party device called the Internet of Things Security Support Provider (IoTSSP) and two main mechanisms for 6LoWPAN Border Router (6LBR) to redirect the DTLS handshaking to the IoTSSP

Kothmayr et al. in [46] described IoT security solution. They proposed the use of dedicated hardware to enable security in constrained devices. The main idea is to use the trusted-platform modules (TPM) added to each constrained device. Although this hardware supports RSA, the most widely used public key cryptography, and works on top of the standard low power communication stacks, it does not endorse CoAP recommendation of using ECC cryptography. Furthermore, the proposed architecture provides message integrity, confidentiality, and authenticity with affordable energy, end-to-end latency and memory overhead, which make it a feasible security solution for the emerging IoT.

Xin described a mixed encryption algorithm used in IoT security transmission [47]. The proposed algorithm provides information integrity, confidentiality, non-repudiation on the data transmission for IoT using the crucial hybrid technology, which takes into account the characteristics of a symmetric key and asymmetric key. Encryption is a required step for

the security of the Internet of things. The Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) are broadly used for information security. The proposed algorithm uses AES algorithm encryption for its simplicity, velocity, and reliability.

Leo et al., in [48], proposed an architecture model mainly devoted to deploying and managing a federated environment for authority delegation mechanism, identity-based capability and dynamic context information. The primary element of the proposed solution is the Secure Mediation GateWay (SMGW) that is dedicated to managing the secure communication for both intraSGMW and interSMGW nodes, under the assumption that the IoT space can be divided into the intraSMGW and interSMGW categories

3. Information Security Survey

Information security, sometimes shortened to InfoSec, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take (e.g., electronic, physical). Information security's primary focus is the equal protection of the confidentiality, integrity, and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity.

In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes. While similar to "privacy," the two words are not interchangeable. Instead, confidentially is a component of privacy that implements to protect our data from unauthorized viewers. Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals [49]

In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a particular case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically provide message integrity in addition to data confidentiality.

3.1 Information Security in Cloud Computing

Cloud computing emerges as a computational model on the internet as well as distribution design. Its main goal is secure and quick data storage for sensitive information. Cloud computing supports ubiquitous, appropriate, network access to a united pool of resources, i.e. servers, storage, networks, services, and applications. Cloud Computing is a widely used technique for data storage on-demand but involves risk such as data security, privacy protection, access-control and data confidentiality. The present study is a survey of the popularly used encryption techniques that are helpful to secure sensitive information on the cloud. A discussion of the fundamental challenges and issues/characteristics of cloud computing has been done. Identification of security and privacy issues within this framework are highlighted.

Study of the widely used encryption techniques helpful in securing sensitive information on the cloud is debated. The scope has been set for academicians and researchers. Diverse versions of the encryption techniques surveyed and analyzed to identify optimization

features for cloud security.

Amlan jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim and Hoon Jae Lee[50], focused on security user authentication issue. This paper proposed the robust two-step user authentication process where the user is verified before entering into the cloud. Even user can change his/her password whenever it is required. This technique restricts many attacks like denial of service, and it provides efficiency to cloud computing

Ari Juels, Alina opera[51], proposed the framework that secures cloud data by integrity and verification for data availability. A major obstacle in cloud computing is to obtained security and operational risks, i.e. hardware failure, malware, software bugs etc. So, protected for outsourced data on the cloud is necessary. There is also another issue in public clouds is availability and reliability assurances. Mariana Carroll, Alta van der Merwe and Paula Kotzé[52], focused easing for cloud security risk as a necessary step to ensure secure cloud environment. It provided an overview about the cloud computing security risks, i.e. attention to ensure about integrity, completeness, and availability of data as well as benefits that help to build standards, processes, and controls include data security, logical access, network security, physical security and compliance.

Deyan Chen and Hong Zhao[53], analyzes the data security and privacy protection issues in cloud computing. Because of these issues, much large organization still don't share their data on the cloud. Privacy protection is shared data with protecting personal information. The most fundamental challenges are access control and separation of sensitive data. This paper proposed different techniques to ensure access, i.e. fine-grained access authorization. Nirmala, R. K. Shivanadhan and R. Shanmuga Lakshami[54] focused the inactive information's arrangement security is to be done by encoding the information or data and send it to a server that's how confidentiality and integrity of data are implemented by encoding the data. Further, the general idea of distinguishing security issues that influences the cloud environment and related work that are done in the territory of truthfulness are discussed.

The advantage of such act is to have data access to only approved customers or owners as presented by Arockiam, L.; Monikandan, S. [55]. Encryption with obscurity; both concepts are exclusive for securing information in storage management. Obstruction is a process which masquerades unauthorized clients by implementing an exact numerical capacity or utilizing programming techniques. Encryption is the procedure of changing over the comprehensible content into mixed up structure utilizing a calculation and a key. The disorder is same as encryption. Applying encryption and muddling systems on the cloud information will give more assurance against unapproved usage of data.

Kavuri, S.K.S.V.A.; Kancherla, G.R.; Bobba, B.R.[56] presented that client can gain focused information. Such as reports, media or another sort of proofs utilizing outsider produced validation key. For reducing the security issues of cloud computing servers; advance message based confirmation process is defined. It is the process only approved users can have access to data by identifying his/her identity using message uprightness.

Kaur, R.; Singh, R.P. [57], discussed to secure the level of distributed storage security a security model is proposed having three stages private, public, and hybrid. Some encryption techniques are implemented on these three stages to cover areas regarding security factor. Two-tier security structural arrangement for a hybrid. Decoding and encryption techniques for public stage and last the exclusive token era instrument is implemented for the special stage. All these give an advantage of enhancing security, integrity in cloud computing.

Rajani Kanth Tuvalu, Lakshmi Mundane [58], Privacy, trust, access control are the key factor for maintaining security in cloud computing. Distributed computing has many benefits regarding sharing data among untrusted users. The granularity of access control with a successful encryption technique is explained and discussed. Furthermore different access control models for disseminated computing are examined.

3.2 Information Security in Big Data

Today the information security (IS) of data mining is the crucial and comprehensive issue for organizations of the different spheres and size. The main challenges of Big Data IT are the management of large amounts of heterogeneous information and providing its availability. Big Data protection against unauthorized access and corruption (keeping its confidentiality and integrity), as well as availability maintenance, form the key research priorities in this field. The issues related to providing these Big Data features are considered in the paper. The existing approaches to their solution are analyzed. Some concepts for their improvement while designing the secure Big Data mining algorithm are formulated by IS properties.

Using the technology of Big Data collecting and mining increased significantly over the past decade. This is because a significant amount of data is generated in the daily activities of the various organizations and, hence, the volume of organizational information resources grows dramatically.

On the other hand, the violations of IS and its separately allocated subdomain — cybersecurity — is a serious problem for organizations in recent years. Attackers find more sophisticated ways to penetrate the corporate networks (intranets), discovering the Ir new vulnerabilities that were not eliminated promptly. Modern perimeter and its endpoints protection does not guarantee the defense of the entire network and, as a consequence, its users, provided services, and information resources are subjected to the great IS risks

J. Chen and F. Tian developed a system called NiagaraCQ, which made it possible to respond to repeated requests to the database (DB) in larger-scale systems [59]. In such systems, many requests are identical. By thorough similar queries grouping, one can reduce the number of the necessary computing and communication resources, which to some extent solves the problem of data availability. The adaptive scheme of increasing query grouping is applied in the NiagaraCQ system that is used to find the optimal mapping between every new request and the group, in which this request can be included

Another approach to providing access to Big Data network was described by C. Olston and J. Widom [60]. The presented distributed model has nodes, using which the data stream is sent to the central unit, being responsible for the processing of all the incoming requests. At some time, the volume of data destined to the central unit becomes too large. To avoid this situation, the authors propose to set filters that limit the data transfer rate from the separate network nodes. However, this technique allows the request is responding with some approximation (because not all the requests are processed) and, therefore, only works in cases that do not require a high query processing precision.

D. Estrin and R. Govindan proposed technique and show how decomposable function of minimum, maximum, mean, sum and count can be calculated concerning the network architecture [61]. The architecture in this context consists of three components: collectors, analyzers, and dumps. The collectors gather information about the network attributes (for example, the number of nodes), which are calculated continuously, periodically or upon the

occurrence of specific events (described as an exception in a trigger). The analyzers are used at the moment when the network issue reports are sent from the collectors for subsequent scanning of network resources.

H. Kargupta work [62] use the results of the matrix perturbation theory and spectral analysis of large random matrices for searching the filtering method of random additive noise. The authors show that when the noise variance takes a sufficiently small value, and the original data have correlated components, then the spectral filtering of the covariance matrix can reveal the original data with reasonable accuracy. However, this method is subjected to the known-sample attack where the attacker has multiple independent samples from the initial data distribution and assumes that the perturbation matrix is orthogonal.

3.3 Information Security in Wireless Network

This section will describe a survey of information security issues in wireless networks from a novel perspective. It figures out information security issue inherent to wireless networks because of their design simplicity. Distributed Denial of Services (DDoS) in its various forms is being increasingly used as a type of attack, with the advent of technical expertise DDoS has been camouflaged into forms more devastating and more difficult to mitigate. There are specific motivational factors for attackers that need to be focused on a comprehensive defense mechanism.

Piyush *et al*. has given approach where the source and destination nodes undertake end to end verification to check if destination nodes intended has received packets transmitted or not [63]. On detecting anomalous behavior, network initiates procedures for finding malicious nodes. The strength of the phenomenon lies in the condition that each node is surrounded by more trusted nodes than malicious nodes which are not always a reality.

Chen *et al*. proposed an approach relying on two related algorithms viz. key management algorithm that incorporates gossip protocol and Detection algorithm utilizing aggregate signature [64]. Here every node, part of the session has to make a proof of received messages. On suspecting some anomalous behavior, the source may initiate checkup process for nodes in the pathway, based upon data returned by checkup process; it (source node) traces the compromised node with the help of diagnostic algorithms. The computational cost of this approach is a little bit high because of methods of detection viz. gossip protocol and aggregate signatures.

Slightly less effective but straightforward approach is proposed by Arshad *et al*. which uses passive acknowledgment in its pure form [65]. Promiscuous mode of the communication channel is utilized which enables all nodes to check any transmitted packet no matter to whom it is intended for, ensuring sender nodes that packets they have sent to their neighbors for forwarding are in fact forwarded.

Ming-Yang *et al*. have proposed a grading method for nodes by ABM (Anti Blackhole Mechanism), in ABM nodes are evaluated for suspicious value; suspicious values are the difference of RREQ, and RREP counts for a given node [66]. Here all node perform ABM, and intermediate nodes are debarred from replying to RREQs, so if there is a node neither destination nor source and never broadcast RREQ for a specific route, but forwards an RREP for the specific route, its suspicious index is raised in the neighboring nodes abnormal table. Eventually, when suspicious index bypasses a threshold, a block message is generated by this neighboring node to all other nodes of the network to isolate this node.

Shukla *et al*. proposed a framework[67]. In the framework, starting actual communication source sends some prologue messages to destination making it aware that there is a communication to be started for it, at the end of communication destination nodes repeats this procedure to inform about number of packets received by it; if the no. of packets lost exceeds the acceptable range limit, the process of malicious node discovery is started by accumulating responses from monitoring nodes and networks.

Oscar *et al*. have used an algorithm that is based on the principle of flow conservation and accusation of nodes for their behavior. Here certain threshold defines well-behaving nodes and misbehaving nodes. However, based upon this approach a network cannot be made misbehaving nodes free as ascertaining nodes behavior has time complexity involved, and a node can have misbehaved before data being accumulated for its behavior [68].

Ahmad Tariq has proposed a 4 step technique to detect and isolate malicious node and to ensure that it cannot be a part of any communication anymore. This technique relies upon two detection procedures viz. local and cooperative detection models for identification of malevolent nodes[69].

One of the earliest studies on trusted routing was undertaken by Marti et al. [70]. Their approach consisted of 3 parts viz. the routing protocol, pathrater component and a watchdog component. The watchdog component determines if a neighboring nodes' actions are according to normal behavior or are deviating from the protocol (e.g., not forwarding packets, tampering with packets, etc). This information was fed to pathrater component to determines the quality of routes which subsequently help router component to make proper route decisions.

Vicente Segura, Javier Lahuerta have conducted a study on economic incentives of DDoS attack. In their study they have first tried to understand the factors affecting DDoS attackers and then proposed an economic model for it. They have given a mathematical model also to assess the economic incentive of an attackers and consequently have applied it as well on some survey data collected by themselves [71].

Liu et al. have made an effort to model attackers' psychology, their goals for attack and their strategy to counter the effects of attack and predict a robust, proactive model for Cyberdefense [72]. Fultz et al. have proposed their model based on game theory, in which attacker is trying to infiltrate the security system to deny services whereas defenders are simultaneously trying hard to seize their effort. The study shows that only threat of criminal prosecution is enough to distract attacker from attacking however with increasing number of attackers system becomes imbalanced [73].

These issues are inherent in wireless networks because of their flexible nature and openness. Out of various issues related to wireless networks confidentiality is concerned with Authorization, authentication and use of robust encryption algorithms. Integrity in wireless networks is relatively easy to compromise but available mechanism viz. Checksum etc. to protect integrity is enough for protection of data integrity. Availability indeed is an aspect of security issue which remains a challenge for research communities and professionals. DoS, DDoS, Blackhole, Grey hole, etc. are forms of attacks being used increasingly and frequently day by day. We have tried to look into motivation factors of attackers as well; a broad classification is also presented to model intentions/ incentives of the attacker and their psychology.

4. Conclusion

In this paper, we will present a lot of approaches to solving Networks and Information Security issues. We survey network security in LTE technologies, Vehicular Ad-Hoc Network, and security in Wireless Sensor Network. Internet of Things. In this paper, we describe many methods in Information Security. Is consist of Information Security in Big Data and Cloud Computing.

References

1) S. D. Krit and E. Haimoud, ``Review on the IT security: Attack and defense,'' in Proc. Int. Conf. Eng. MIS, Agadir, Morocco, 2016,
2) F. Sabahi and A. Movaghar, ``Intrusion detection: A survey,'' in Proc. 3rd Int. Conf. Syst. Netw. Commun., Sliema, Malta, 2008, pp. 2326.
3) W. Xu, W. Trappe, Y. Zhang, and T. Wood, ``The feasibility of launching and detecting jamming attacks in wireless networks,'' in Proc. ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2005, pp. 4657.
4) A. G. Fragkiadakis, V. A. Siris, and A. P. Traganitis, ``Effective and robust detection of jamming attacks,'' Future Netw. Mobile Summit, 2011,
5) M. Lichtman, T. Czauski, S. Ha, P. David, and J. H. Reed, ``Detection and mitigation of uplink control channel jamming in LTE,'' in Proc. MILCOM, 2014, pp. 1187-1194.
6) J.-H. Bang, Y.-J. Cho, and K. Kang, ``Anomaly detection of networkinitiated LTE signaling trafc in wireless sensor and actuator networks based on a Hidden semi-Markov model,'' Comput. Secur., vol. 65, pp. 108-120, Mar. 2017.
7) R. Bassil, A. Chehab, I. Elhajj, and A. Kayssi, ``Signaling oriented denial of service on LTE networks,'' in Proc. ACM Int. Symp. Mobility Manage. Wireless Access, 2012, pp. 153-158
8) A. Gupta, T. Verma, S. Bali, and S. Kaul, ``Detecting MS initiated signaling DDoS attacks in 3G/4G wireless networks,'' in Proc. Int. Conf. Commun. Syst. Netw., 2013, pp. 160.
9) M. Pavloski, G. Görbil, and E. Gelenbe, ``Bandwidth usageBased detection of signaling attacks,'' Inf. Sci. Syst., vol. 363, pp. 105114, Sep. 2015.
10) S. Wahl, K. Rieck, P. Laskov, P. Domschitz, and K. R. Müller, ``Securing IMS against novel threats,'' Bell Labs Tech. J., vol. 14, no. 1, pp. 243257, 2009.
11) M. Nassar, R. State, and O. Festor, ``Monitoring SIP trafc using support vector machines,'' in Proc. Int. Workshop Recent Adv. Intrusion Detection, 2008, pp. 311330.
12) D. Seo, H. Lee, and E. Nuwere, ``SIPAD: SIP-VoIP anomaly detection using a stateful rule tree,'' Comput. Commun., vol. 36, no. 5, pp. 562574, Mar. 2013.
13) S. Zhang, L. Zhou, M. Wu, Z. Tang, N. Ruan, and H. Zhu, ``Automatic detection of SIP-aware attacks on VoLTE device,'' in Proc. IEEE Veh. Technol. Conf., Sep. 2016, pp. 15
14) J. Lee, K. Cho, C. Lee, and S. Kim, ``VoIP-aware network attack detection based on statistics and behavior of SIP trafc,'' Peer-to-Peer Netw. Appl.,vol. 8, no. 5, pp. 872880, Sep. 2015.
15) Z. Bin et al., ``Behavior analysis based SMS spammer detection in mobile communication networks,'' in Proc. IEEE DSC, Jun. 2016,
16) C. Wang et al., ``A behavior-based SMS antispam system,'' IBM J. Res. Develop., vol. 54, no. 6, pp. 3:13:16, Nov./Dec. 2010.
17) A. Modupe, O. O. Olugbara, and S. O. Ojo, ``Filtering of mobile short messaging service communication using Latent Dirichlet allocation with social network analysis,'' in Power Technology and Engineering, Dordrecht, The Netherlands: Springer, 2014, pp. 671686
18) Hong, Xiaoyan, Dijiang Huang, Mario Gerla, and Zhen Cao, "SAT: situation-aware trust architecture for vehicular networks", In Proceedings of the 3rd international workshop on Mobility in the evolving internet architecture, pp-31-36, ACM, 2008.
19) Hortelano, Jorge, Juan Carlos Ruiz, and Pietro Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in vanets", In Communications Workshops (ICC), IEEE International Conference on, pp- 1-5. IEEE, 2010
20) Liao, Cong, Jian Chang, Insup Lee, and Krishna K. Venkatasubramanian, "A trust model for vehicular network-based incident reports", In Wireless Vehicular Communications (WiVeC), IEEE 5th International Symposium on, pp-1-5, IEEE, 2013.
21) Wang, Zhou, and Chunxiao Chigan, "Countermeasure uncooperative behaviors with dynamic trust-token in VANETs", In Communications, ICC'07, IEEE International Conference on, , IEEE, 2007.
22) Biswas, Subir, Jelena Misic, and Vojislav Misic, "ID-based safety message authentication for security and trust in vehicular networks", In Distributed Computing Systems Workshops (ICDCSW), 31st International Conference on, pp- 323-331. IEEE, 2011.
23) Gazdar, Tahani, Abderrezak Rachedi, Abderrahim Benslimane, and Abdelfettah Belghith, "A distributed advanced analytical trust model for VANETs", In Global Communications Conference (GLOBECOM), IEEE, pp- 201-206. IEEE, 2012.

24) Wei, Yu-Chih, and Yi-Ming Chen, "An efficient trust management system for balancing the safety and location privacy in VANETs", In Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th International Conference on, pp- 393-400. IEEE, 2012
25) Gómez Mármol, Félix, and Gregorio Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks", Journal of Network and Computer Applications 35 springer, no. 3 pp- 934-941,2012.
26) Gazdar, Tahani, Abderrahim Benslimane, and Abdelfettah Belghith, "Secure clustering scheme based keys management in VANETs", In Vehicular Technology Conference (VTC Spring), IEEE 73rd, pp- 1-5. IEEE, 2011.
27) Ding, Qing, Xi Li, Ming Jiang, and XueHai Zhou, "Reputation-based trust model in vehicular ad hoc networks", In Wireless Communications and Signal Processing (WCSP), International Conference on, pp- 1-6, IEEE, 2010.
28) Gazdar, Tahani, Abderrahim Benslimane, Abderrezak Rachedi, and Abdelfettah Belghith, "A trust-based architecture for managing certificates in vehicular ad hoc networks", In Communications and Information Technology (ICCIT), International Conference on, pp180-185.,IEEE, 2012.
29) Chen, Yi-Ming, and Yu-Chih Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs", Communications and Networks, Journal of 15, no- 2 pp- 153-163, 2013.
30) Chen, Chen, Jie Zhang, Robin Cohen, and Pin-Han Ho, "Secure and efficient trust opinion aggregation for vehicular ad-hoc networks", In Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd, pp. 1-5. IEEE, 2010.
31) Sahoo, Rashmi Ranjan, Rameswar Panda, Dhiren Kumar Behera, and Mrinal Kanti Naskar, " A trust based clustering with Ant Colony Routing in VANET", In Computing Communication & Networking Technologies (ICCCNT) Third International Conference on, pp- 1-8. IEEE, 2012.
32) Amee A. Patel, Sunil J. Soni, "A Novel Proposal for Defending Against Vampire Attack in WSN", IEEE Fifth International Conference on Communication Systems and Network Technologies, 2015.
33) Chen Hongsong, Han Zhi, Fu Zhongchuan, "Quantitative Trustworthy Evaluation Scheme For Trust Routing Scheme in Wireless Sensor Networks", *IEEE Trustcom/BigDataSE/ISPA*, pp. 1272-1278, 2015.
34) S. Prachi, Piyush Moon, K. Ingole, "An Overview on: Intrusion Detection System with Secure Hybrid Mechanism in Wireless Sensor Network", *IEEE International Conference on Advances in Computer Engineering and Applications (ICACEA)*, pp. 272-277, 2015.
35) Neeraj Khanna, Joel James, Joyshree Nath, "New Symmetric Key Cryptography Algorithm using Combined Bit Manupulation and MSA Encryption Algorithm: NJJSA Symmetric Key Algorithm", *Proceedings of CSNT-2011 held at SMVDU (jammu)*, 03–06 june 2011.
36) Somdip Dey, Asole Nath, MES-1 (modern encryption standard) an advanced cryptography method, IEEE, 2012.
37) Lina R. Deshmukh, A. D. Potgantwar, "Ensuring an Early Recognition and Avoidance of the Vampire Attacks in WSN using Routing Loops", *IEEE International Advance Computing Conference (IACC)*, 2015.
38) Boqing Zhou, Jianxin Wang, Sujun Li, Yun Cheng, Jie Wu, "A Continuous Secure Scheme in Static Heterogeneous Sensor Networks", *IEEE Communications Letters*, vol. 17, no. 9, September 2013.
39) Eugene Y. Vasserman, Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", *IEEE Transaction on Mobile Computing*, vol. 12, no. 2, February 2013.
40) Harsh Kumar Verma, Saurabh Singh, "security for wireless sensor networks", *International Journal on Computer Science and Engineering (IJCSE)*, vol. 3, no. 6, June 2011.
41) Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah, Kashif Naseer Qureshi, "Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks", *IEEE International Conference on Smart Sensors and Application (ICSSA)*, 2015.
42) R. Tahir, H. Tahir, K. McDonald-Maier, A. Fernando, "A novel ICMetric based framework for securing the Internet of Things", *2016 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 469-470, 2016.
43) C. Liu, Y. Zhang, H. Zhang, "A Novel Approach to IoT Security Based on Immunology", *Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security*, December 2013.
44) L. Zhou, H. C. Chao, "Multimedia traffic security architecture for the internet of things", *IEEE Network*, vol. 25, no. 3, pp. 35-40, May-June 2011.
45) G. Lessa, dos Santos, V. T. Guimarães, G. da Cunha Rodrigues, L. Z. Granville, L. M. R. Tarouco, "A DTLS-based security architecture for the Internet of Things", *2015 IEEE Symposium on Computers and Communication (ISCC)*, pp. 809-815, 2015.
46) T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, G. Carle, "DTLS based security and two-way authentication for the Internet of Things", *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710-2723, 2013.
47) M. Xin, "A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System", *2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 62-65, 2015.
48) M. Leo, F. Battisti, M. Carli, A. Neri, "A federated architecture approach for Internet of Things security", *2014 Euro Med Telco Conference (EMTC)*, pp. 1-5, 2014.
49) Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress. p. 240. ISBN 9780128008126.

50) Amlan jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim and Hoon Jae Lee “A Strong User Authentication Framework for Cloud Computing” *2011*
51) Ari Juels and Alina opera “New Approaches to Security and Availability to Cloud Computing” *ACM-RSA laboratories, 2013*
52) Mariana Carroll, Alta van der Merwe and Paula Kotze“Secure Cloud Computing Benefits, Risks and Controls” *IEEE-Information Security South Africa, 2011*
53) Deyan Chen and Hong Zhao “Data Security and Privacy Protection Issues in Cloud Computing” *IEEE-Conference on computer scienceand electronic engineering, 2012*
54) V. Nirmala, R. K. Shivanadhan and R. Shanmuga Lakshami “Data Confidentiality and Integrity Verification using User Authenticator scheme in Cloud” *pp. I-5*
55) Arockiam, L., Monikandan and S. “Efficient cloud storage confidentiality to ensure data security” *pp. 1-5-3-5, Jan 2014*
56) Kavuri, S.K.S.V.A., Kancherla, G.R., Bobba and B.R. “Data authentication and integrity verification techniques for trusted/untrusted cloud servers” *Conference in Advances in Computing, Communications and Informatics, pp. 2590-2596, Sept., 2014*
57) Kaur, R., Singh and R.P. “Enhanced cloud computing security and integrity verification via novel encryption techniques” *pp. 1227-1233, 24–27 Sept. 2–14*
58) Aluvalu, R., Muddana and L. “A Survey on Access Control Models in Cloud Computing” *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI), vol. 1, pp. 653-664, 2015, Springer International Publishing*
59) J. Chen, D. DeWitt, F. Tian, Y. Wang, "NiagaraCQ: a Scalable Continuous Query System for Internet Databases", *Proceedings of SIGMOD'00 Dallas Texas*, pp. 379-390, 2000.
60) C. Olston, J. Jiang, J. Widom, "Adaptive Filters for Continuous Queries over Distributed Data Streams", *Proceedings of SIGMOD'03*, pp. 563-574, 2003.
61) R. Govindan, D. Estrin, "Computing Aggregates for Monitoring Wireless Sensor Networks", *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 139-148, 2003.
62) K. Liu, C. Giannella, H. Kargupta, "An attacker's view of distance preserving maps for privacy preserving data mining", *Proceedings of PKDD '06*, September 2006.
63) Piyush Agrawal, R. K. Ghosh, Sajal K. Das, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", *2nd International Conference on Ubiquitous Information Management and Communication*, pp. 310-314, 2008.
64) ChenWei, Long Xiang, Bai Yuebin, Gao Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks", *Second International Conference on Communications and Networking in China*, pp. 366-370, 2007.
65) Arshad Jhumka, Nathan Griffiths, Anthony Dawson, Richard Myers, An Outlook on the Impact of Trust Models on Routing in Mobile, 2008.
66) Ming-Yang Su, "Prevention of Selective Black hole Attacks on Mobile Ad hoc Networks through Intrusion Detection Systems", *Computer Communications*, 2010.
67) Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", *World Congress on Engineering and Computer Science*, pp. 337-342
68) Oscar F. Gonzalez, Godwin Ansa, Michael Howarth, George Pavlou, "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks", *Journal of Internet Engineering*, vol. 2, no. 1, pp. 181-192, 2008.
69) Tariq Ahamad, "Detection and Defense Against Packet Drop Attack in MANET", *International Journal of Advanced Computer Science and Applications(IJACSA)*, vol. 7, no. 2, June 2016.
70) S. Marti, T. J. Giuli, K. Lai, M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", *Proceedings of the 6th annual international conference on Mobile Computing and Networking (MOBICOM)*, pp. 255-265, 2000.
71) V. Segura, J. Lahuerta, T. Moore, D. Pym, C. Ioannidis, "Modeling the Economic Incentives of DDoS Attacks: Femtocell Case Study" in Economics of Information Security and Privacy, Boston, MA:Springer, 2010.
72) P. Liu, W. Zang, M. Yu, "Incentive-based modeling and inference of attacker intent objectives and strategies", *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 1, pp. 78-118, February 2005.
73) N. Fultz, J. Grossklags, Roger Dingledine, Philippe Golle, "Blue versus Red: Towards a Model of Distributed Security Attacks In Financial Cryptography and Data Security" in Lecture Notes in Computer Science, Berlin, Heidelberg:Springer-Verlag, vol. 5628, pp. 167-183, 2009