Context - Aware Information Security in the World of Big Data

Dr. Nitin Varma
Professor
Chitkara University
Chandigarh, Punjab, India.

Prof. Pradip Kumar Bala
Area Chair
Analytics an Information Systems
Indian Institute of Management Ranchi
Ranchi, Jharkhand, India.

Abstract

For the first time computer launched foreign assaults on U.S. infrastructure were ranked higher in the U.S. intelligence community's annual review of worldwide threats than worries about terrorism (Dilanian, 2013). That alone speaks volumes about the importance and critical need for information security management – for national as well as international security.

As the world heads towards the massive penetration of internet through mobiles and IOT (Internet of Things) and as the world ultimately transitions from early-Pervasive to Ubiquitous computing, the internet and therefore information security are bound to be massively and inextricably enmeshed with human existence, while multiplying by many orders of complexity, sensitivity and criticality.

Security awareness itself is an issue with 70% global organizations (Deloitte, 2017), one of the key reasons being- lack of a concise yet comprehensive and contemporary information security context. This paper traverses the vast landscape of information security quickly to construct and provide a first ever big picture of the contemporary information security context while providing an eye-opening discussion of what are thought of as "current safe information security practices". This work further finds that though not widely known yet - existing paradigms, already insufficient to provide sustainable information security, are going to fall woefully short either on protection or coverage, or even be rendered obsolete. Taking cues from the shortcomings pointed out by early Big Data practitioners, the paper recommends the use of context-aware Big Data practice for security analytics and discusses how the Big data-6C paradigm may help. The importance of machine learning for delivering context and context-awareness, is emphasized, to emerge with a set of potential winning approaches centering on malbehavior prevention and resilience. The first ever contextual framework for malbehavior that may serve as the core of context-aware

security systems, and a wider Cyber-Physical contextual framework that may provide sustainable information security, are also proposed.

Keywords

Context Aware Security, Sustainable Information Security, Pervasive Computing, Ubiquitous Networks, Big Data Analytics for Security, Metadata for Context Development.

1. Information Security: Issues, Advances and the New

Information security has been like the elephant in the room – albeit the one that is moving in the room, and being looked at, from the keyhole: so, it seems to be revealing a new aspect, every-time. Therefore, it is difficult to understand the comprehensive context and there never has been an attempt to understand the history of security (Leuuw, 2007) and there has been no recent attempt either, to construct a comprehensive contemporary context for information security.

In the initial days information security experts focused more on transmitting 'x' number of internet packets "securely" from one point and receiving the same 'x' number of packages at the intended destination.

Later it began to emerge that internet packets they were prone to manipulation in transit, i.e. internet packets could be subject to various manipulations, including – the contents could be altered, contents could be viewed on the way and therefore be even "copied", they could be re-routed, or they could even be delayed or completely prevented from being delivered. Since internet packets are "written" in software and due to percolation of the skills required, for almost a song, amidst the actors- the information packet has become an alterable "cricket" ball - which could rather quietly be tampered with.

This compared to nature were at the atomic level fundamental constituents cannot be altered by just anybody without sophisticated, usually very expensive, usually conspicuous (requiring huge physical facilities) and intensive (cannot exist without drawing considerable resources from nearby settings) set-up. The sense of security in IT industry is therefore belied by the corruptibility of the fundamental particle of the internet, the "internet packet" that even eight-year olds have demonstrated can be so easily impregnated.

While the OSI model and TCP/ IP hardened, not too later, with the emergence of "hackers" (1960s, MIT) out from the grays into formal

existence – the information security world changed forever. The IT honchos always knew "it", and so now did the public – as the awareness of the "inherent" information security risks spread.

The internet, the unencrypted and unsecured version of it that has grown like wildfire, today looks more like a river flowing in the open, all across the world with infinitesimal distributaries (that carry its contents far and wide in various directions to consumers and beneficiaries) and tributaries (that bring in it from contributing sources – many of them suspect and polluting - deliberate or otherwise). The question of information security therefore has become a challenge akin to preventing some random persons, animals, non-living objects or even air particles from polluting this river as it flows across countries and continents with its countless tributaries and distributaries, amidst thick populace of all types, out in the open. The predictability of such a security scenario can only be the other extreme of being "absolutely secure" - it is clear this challenge requires a far more encompassing and integrated yet deeper strategy.

Since the enterprise user's awareness and threat perception could lead to slower or non-adoption of the internet and computing, several user-end security approaches were devised to aspire confidence. As long as the user felt they had some "degree of control" over their security, to threats posed by hackers, including ethical threats, businesses could push forward with computerization by "raising the barriers to entry" through providing users the following security options, depending upon system maturity and capabilities:

1. **User exclusivity:** authorized users were only to be "supported", including through multiple factor authentication, i.e. through bio-metrics or through two-step verification (password and code sent to mobile etc.).
2. **User type:** basic user types were defined - e.g. guest, business, administrator were "supported".
3. **User profile:** advanced user types in terms of more sharply defined job functions, IT requirements and apps eco-system were to be granted "official access" and were to be "supported".
4. **User privileges:** far more granular enablement of user functions defined privileges - do's and don'ts were permitted to each user without providing broad/sweeping permissions.

5. **Automated No-Activity No-Access Zones:** these virtual and even physical zones kept the average user away, so that they would not be the risk themselves, or would be kept away from a set of pre- assessed threats using automated no-activity, detection and quarantine tools.
6. **Activity Risk Assessment:** based on activities being carried out by user on the computer. Since this level of security starts being quite intrusive, people in powerful positions and with the right contacts in IT often have it set down too low or have it waived off completely, therefore leaving a gaping hole in security.

The above enterprise approach to internet and security in general, enabled considerable percolation of the "impervious internet" thought – at least temporarily, into most new human entrants that started working in the IT industry, or with a computer at the job. Most new entrants believe the "internet is secure" with enterprise adopted security – and that trying to beat the system will take a lot of effort and pain. Couple that with emerging stronger e-commerce laws specific to enterprise computing, the game was set. The average user believed it was pointless to even "try to break the security". The enterprise, in other words, had thus been successful in setting up the "first barrier to entry" (to threats).

However, the irony early-on being that "authorized users" were hardly thought of being capable of becoming carriers of the risk themselves, even if considered intrinsically benign – or at least that was the thought conveyed to the masses. It must be noted that the attention enterprise security needs received from the industry far preceded and exceeded the needs for personal information security. In the security industry, there was a strange black hole that never threw back an answer to the question "Authorized users – we know at least something. What about others?" Authorization and access were to be controlled at the organization level to accomplish several tasks, driven more by the needs of the enterprise rather than the need for global information security, though those did aid information security to varying impact:

- by somewhat insulating the digital organization from vulnerabilities in the global internet
- by creating privileged access and through administration of privileges, for access to the organization's digital assets
- by managing traffic and consumption of the functions of the digital organizational only for the betterment of the organization and not for the individual's unauthorized gain

- by preventing this "new" digital organization from becoming an "easy" contaminant tributary to the internet, in general. One voluntary lesson sure had been taken – all "new" entrants to the internet eco- system were to be set-up in such a way that they would not easily turn contaminants once connected to the main internet pipe
- by taking measures to safeguard the global growing organization from any legal issues arising from adoption of computing and internet at locations far and wide, especially to prevent "careless" use of internet at the hands of an ignorant or anti-element, that could embroil the enterprise in threatening and potentially even billion dollar lawsuits and therefore be disruptive to business, in territories and regions beyond the organization headquarters.

Mass adoption of the above approach eventually also brought to fore its own limitations. Since first and foremost, most of the mass information security approaches start with a circle of influence – the above approach and many current practices along the same lines apply to only those people or entities that enter or assert themselves within this circle of influence. A solitary threat outside this rather limited circle of influence may not be governed and managed by the above security practices, and therefore continues to be a threat, albeit often even an undetected one till the damage is done and is often widespread – consequence of little information sharing or integrated action. Of late, cases of information security transcending its "soft nature" and manifestation of the security threat in immensely damaging physical forms- like powerhouse outages, mis-functioning of flight information systems resulting in flight schedules going haywire and so on have become evident. This despite data encryption, data masking and a slew of technological advancements aimed at enhancing what has turned out to be most valuable in the information security paradigm: data – both business and personal, for which, unfortunately, some of the players of the IT industry itself are to blame - for having created a "sell data - get quick rich" market.

To make things even more perilous from the perspective of security, the number of large corporations buying and selling data is expected to go up from the current 70% to 100% by 2019– effectively making data itself a huge market. IOT (the Internet of Things) will be the next critical focus for Analytics. It is also expected security would become the killer app for Big Data (Press, 2014).

With the advent of IOT, information security is expected to acquire even far more physical and common-place meanings:

- an internet connected refrigerator suddenly goes "down" in a self-care home, with a recuperating person who could have been greatly helped by the automatic food ordering system
- someone or something may be able to corrupt the wireless signal from a mobile phone double-acting as car remote to start-up the air-conditioning and cool-down a car in snow-laden Michigan
- a self-driven car has its instructions corrupted, had been hired to drop a junior-school student, goes haywire and instead of taking exit 1 to school, takes exit 10 to interstate-80 leading to Casinos in Reno In the IOT world, there is no dearth of examples of what security breaches could lead millions of people to, on an hourly basis.

The information security challenge, therefore, will be more pronounced and time-pressed for its ability to predict, if not identify, well-before the occurrence(s): threats, events, security needs and their definitions across environments. Is a certain event, action, or behavior a threat, and can it be defined the same else-where in different contexts?

The task is only going to be made more unmanageable by new less-than-matured IOT devices appearing on the scene from some or the other manufacturer - adding to the security spectrum the issue of inter-activity between the existing and the new (IOT) entrant(s) and the resultant impact on the otherwise and erstwhile stabilized security scenario. The security concept and vulnerabilities of literally every device manufacturer (and its employees) – even if small, and their level of understanding of security- are likely to be at risk of market driven proliferation, like never before (Lampe, 2014).

In the networking world, although transitioning from IPv4 to IPv6 will provide more routing information, the number of devices that is going to be added will make it very big. Though somewhat secure, IPSec is still not an option for the regular mass use. SSL, especially Open SSL- showed it could have a catastrophic Heartbleed, and that too, without any trace log, whatsoever (Codenomicon, 2014).

DNS-based attacks could be mitigated by the use of Domain Name System Security Extensions (DNSSEC). DNSSEC has been around since 2010, but it is still being deployed by only a tiny number of companies. 400 Gigabits per second DDoS (Distributed Denial of Service attacks) were recorded, more than the bandwidth of a small country (Nichols, 2015) and more than

one billion records were breached (Thibodeau, 2015). If these were to be unique individuals, that would mean roughly every sixth person on this planet affected the new workplace – the office, itself is a problem. The workplace is now anywhere and everywhere and at any time. This means the traditional controls that brought in security are gone! Employees not following security policies are the biggest threat to endpoint security (Prince, 2015).

Also the apps on computers and mobile devices in the "new" office, are under no regulation and pose a greater threat as well. Executives say users' slack attitude toward mobile security, and ease and low cost for software development mean mobile apps increasingly are a huge source of risk (Phneah, 2012).

Then there are hardware and software products that just act as conveyer pipes by hosting, ad-hoc internet networks or by providing such surfaces for signal processing. Some of this technology forms the basis of what are called "Smart" devices, though most cheap versions are at the lowest level of security. These can be turned into rogue elements by a slightly skilled person to act as conveyers of security threats of varying types. An Internet-connected fridge was co-opted into a botnet that sent spam to tens of thousands of Internet users (Vijaiyan, 2015).

New programming languages with significantly higher computing abilities, or at times adapted too fast and therefore laden with insecure coding practice, e.g. HTML5, and new evolving forms of malware like APTs (advanced persistent threats) are extremely hard to predict or detect (Teller, 2012).

Microsoft OS, the most installed OS – may innocuously seem like one OS with rather limited versions, however, in reality it may already exist in millions of versions - given the patch level, apps, form factors, hardware and software configuration(s). That can lend a false air of security. A single vulnerability called CVE-2015-0057, involving the modification of only one bit has been found to be capable of hacking all versions of Windows (Kovacs, 2015).

The ease with which data can be stored and ported has brought its own risks. These risks have become so high, especially regarding the current most portable data medium, the USB that the USB has even been called Ultimate Security Breakdown, and the advice for USB definitely is: "use with extreme caution" (Kaplan and Kaplan, 2014).

Social media accounts, the multitude of accounts everyone has of various types, need to have easily re- callable passwords – so passwords are repeated and increase chances of hacking at many places (Bilton, 2013). Though two-factor authentication provides some relief - the price is considerable inconvenience, lack of reliability of second password delivery and the risk of losing it all in certain situations.

Moving to Cloud – may be thought of as secure, though it has its own impact on security. Availability of encrypted log data, 7 years offline and 1 year online – per typical Cloud contracts, makes the Cloud even more attractive to hackers. If a multi-tenant cloud service database isn't designed properly, a single flaw in one client's application could allow an attacker to get at not just that client's data, but every other clients' data as well (Ted, 2013). Context-awareness and cloud have recently become topics of great interest (CFP, 2018).

Alternate secure mass OS? Google's Android operating system averaged 5,768 malware attacks daily over a six-month period, according to CYREN's Security Report for 2013. Attackers continue to search for the weakest point in the chain and after finding one, home in (Collett, 2014).

It is already an era of Designer attacks (IBM 2007). Hackers are no longer throwing mass attacks at all targets. Attacks, specific and necessary to break a particular system are almost common. In the New York Times breach of 2013, investigators from a security specialist firm, Mandiant – after the FBI was no longer able to make a headway, determined that hackers used 45 pieces of custom malware in the attacks against the New York Times over three months, but only one of them was detected by the antivirus products from Symantec used by the newspaper in its systems. To begin with, the NY Times did not even know there was anything fishy, it was AT&T that alerted them (Perlroth, 2013).

Add to that the upcoming field of process analytics and machine data analytics – these propose to extract important predictive information through analytics applied to every single process and piece of machine data, to aid security analytics. Then there are frameworks for compliance like CobiT, ISO 27002:2013, PCI Compliance and others. Then, there still are no definitive answers for many of the security concerns that may have roots in the past. For example, what would be the impact of the waking up of an erstwhile abandoned Y2K era machine in 2025, for example, in a new civilization of the IOTs? All this while the world is already undergoing waves of deeper penetration of PC, laptop, mobile and IOT and other

devices- all with differing concoctions of software, differing interpretations of security - at different paces in different economies – resulting in rather unpredictably variegated, non-homogenous and in equal but humungous potential security relevant "Big Data". The following big picture shows the context for information security - threats and manifestations:

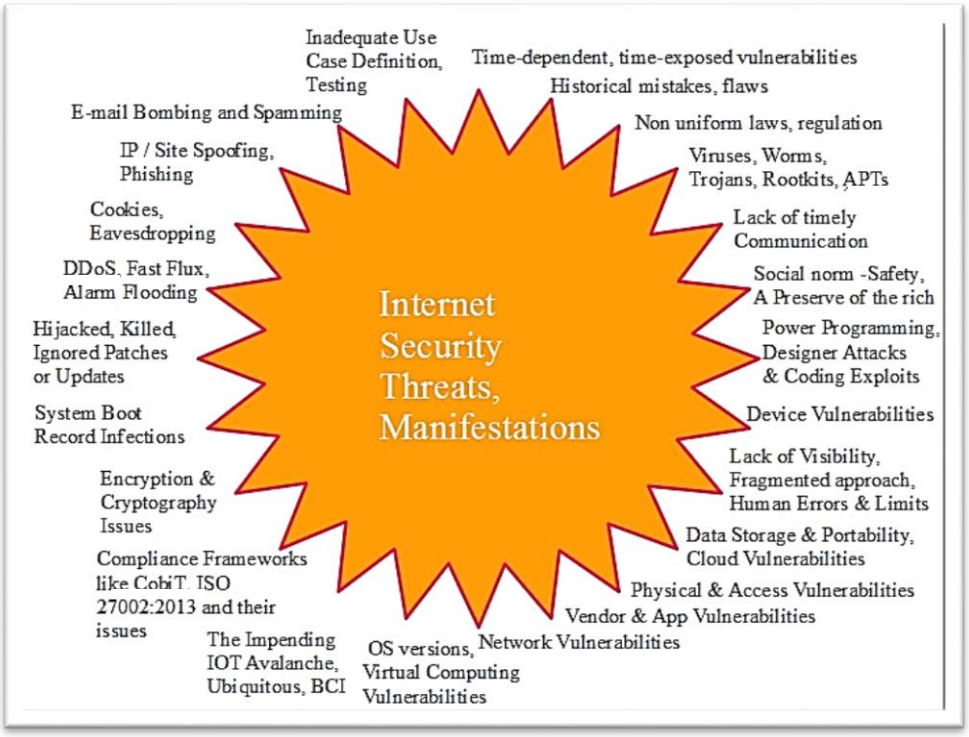

Fig-1 The Big Picture: Information Security Threats, Manifestations

It is clear that the rather discontinuous information security space is undergoing an entropy big bang. With the dawn of air like ubiquitous internet, the term "information security" is bound to broaden and acquire unprecedented scale, meanings, dimensions, complexity, sensitivity and potential for harm. What can security scientists do to manage or to even begin to analyze such internet mayhem?

Given the scale, machines will have to be taught to reduce the humongous amounts of data that is going to be generated, to more human actionable agglomerates. The machines will have to learn to catch the early signs. Therefore, as the world moves from early-pervasive computing to

Ubiquitous computing (McCrory, 2000), information security analytics is going to be the killer area for Big Data Analytics.

2. Enter: Big Data - The Cure and its Ills

Big Data (James et al., 2011) may be defined as "datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze."

Big Data definitions (Grimes, 2013) have attempted to expand beyond the original three V's – volume, velocity and variety to seven V's: volume, velocity, variety, veracity, variability, value and visualization. "Viability" is being said to be the eighth "V".

Upto 80% of business knowledge is believed to be locked in unstructured text (Adrian, 2011). The Time Magazine chose to devote its cover page story to reflect this importance: "Why Text Mining May be the Next Big Thing" (Belsky, 2012). The U.K. (Britain) became the first country to start-up an institute dedicated to text mining, called NaCTeM (National Center for Text Mining, 2013).

The term "Text Analytics" describes (Hobbs, Walker and Amsler, 1982) a set of linguistic, statistical and machine learning techniques that model and structure the information content of textual sources for various purposes – research, analysis and/or intelligence – in public and private domains.

However, the very unstructured nature of Big Data means Big Data may be hardly utilized through direct queries, in its native form. This is well posited by Bill Inmon (Inmon, 2013), often credited to be the father of data-warehousing:

"There are indeed some important simple differences between data. And why are those simple differences important? They are important because everyone is talking about big data today. You know, the kind of data found in Hadoop. Does anyone stop and realize that all data in Hadoop is unstructured and that you can do only the most basic of queries against that data? Something to think about."

In the OCCAM framework floated on the Harvard Blog Network, Fung (2014) points towards lack of capture, lack of controls, presumed completeness, and loss or mixing of contexts – in current Big Data.

Does Big Data capture what it claims to represent? A major issue could be: "is the instrumentation actually capturing the theoretical construct of interest?" (Lazer, Kennedy, King and Vespignani, 2014).

SAS the world's leading data-mining software maker has identified five Big Data challenges (SAS Institute, 2013): (1) meeting the need for speed (2) understanding data in the right context (3) ensuring data quality (4) being able to visualize output in a meaningful manner and (5) dealing with outliers.

True, important "marker" information may be buried deep inside mounds of Big Data and will pose its own challenges at first being discovered, being relevant, being timely and then of being useful. Is there hope even after learning of Big Data Event log management and monitoring mistake made by Neiman Marcus, where 60,000 alerts were triggered but still hackers were able to steal 40 million credit cards data? (Damballa 2014), There were approximately 150,000 alerts triggered in a day at some customer organizations. Which of these point to truly malicious attacks? Even for the world's first long-distance (Shanghai to Beijing: 1200 km), touted as most secure quantum encryption network (Moore, 2014) designed to alert at even one-photon tampering level, will finding that single photon amongst gazillions of photons and discovering repeat patterns - require some Big Data analytics?

The New York Times, quoting experts and spilling the beans of Big Data science discord in the public domain, reported nine issues related to Big Data including issues about combining (Marcus and Davisparil, 2014) data from various sources and thus resultant ill effects, ostensibly due to mixing of contexts, if any. This points towards the dangers inherent in the creation of a concoction of Big Data in the hurry to spot the aberrations in information security.

The Financial Times London (Harford, 2014), in a scathing attack on Big Data analytics, quoted statisticians and industry cases – to point out how lack of understanding (context), for example of Twitter data, can lead to terribly skewed results. Since security analytics can be expected to have rather high sensitivity, this clearly is a warning of the severe-most level regarding rather "lack-of-context" use of Big Data for security analytics.

"Text analytics" by itself is not less fraught with issues already recognized - complexity of encoding and decoding of text: the case of the convict that could not be hanged because the judge put a comma in the wrong place. It has, for a long time been known that text structures depend crucially on what is regarded as "common-sense" knowledge, which despite-or, more likely, because of- its everyday nature is

exceptionally hard to encode and utilize in algorithmic form (Witten, 2005).

Amidst all that Big Data bashing, The Economist (K.N.C., 2014) reaffirmed Big Data analytics still hold value, that Big Data is only going through a natural cycle of necessary hype-busting. However, a recent survey of data scientists published by the CIO Magazine (Olavsrud, 2014), has once again brought out the frustrations of Big Data scientists, regarding linking multi-sourced data, possibilities of loss of context and other issues.

3. The Information Security Data Big Bang and the Need For Machines

The world of information security is undergoing a huge transformation, albeit quietly.

The security firm, Imperva, in 2012, raised a viral controversy by stating that most anti-virus software did not have more than 5% success rate in detecting new threats (Perlroth, 2013).

In 2012, research firm Gartner said that big data analytics will play a crucial role in detecting crime and security infractions. Gartner expects more than 25 percent of global firms to adopt a big data analytics for at least one security and fraud detection use case by 2016 (Kar, 2014). In a January 2013 report, Booz Allen & Hamilton and EMC stated that:

"The dissolution of traditional defensive perimeters coupled with attackers' abilities to circumvent traditional security systems requires organizations to adopt an intelligence-driven security model that is more risk-aware, contextual, and agile."

Booz Allen & Hamilton & EMC (2013) are expecting dramatic changes:

- Big Data Analytics will be necessary to assess risks accurately
- Big Data Analytics will disrupt the status quo in most information security product segments in about two years' time
- Resources who understand business risk and cyber-attack techniques both, will be in demand

Further, Gartner (2014) expects that significant security challenge will remain because of big data created through deployment of myriad devices will drastically increase security complexity. Even data storage requirements will change. As security needs have evolved, so has the need for context-aware analytics and the time period for which data must be stored (Srikanth, 2013).

How will humans manage this big data? Rieck (2011), while exploring computer security and machine learning are enemies or friends, observes: security researchers are swamped by the amount of malicious activity in the Internet. Whether analyzing malicious programs, faked profiles on social networks or web pages of spam campaigns, in many settings there are thousands of data instances per day that need to be analyzed and fit into a global picture of threats. Rieck (2012) concludes that machine learning may be the best friend of humans, for security.

Rieck (2011) further states that machine learning is designed to infer relationships from large volumes of data. The initial algorithms may not outperform a human analyst, but these will definitely allow processing of mounds of data that no human can do, yielding a sub-set of more readily human- assimilable and actionable data. Automatic analysis of malware behavior is possible using machine learning.

While it may look good in theory, does machine learning actually help with data analysis? Damballa (2014) observed their devices contacting an average of 411 million top-level internet domains. Since January 1, 2014, more than 146 million distinct second-level domains daily were observed, of which an average of 700,000 were new. Of those new domains, 55% were only seen on the day in which they first appeared (Damballa, 2014). It is evident, machine learning can help narrow down security focus to a human comprehensible order of magnitude.

4. Context Driven Approaches For Information Security

The English Oxford Dictionary (Oxford, 2015) defines 'Context' as: the circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood. Aboud and Dey (1999) define context as: any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves.

While evaluating the role of contextual information in pattern recognition, Toussaint (1978) concludes: Contextual information is important for pattern recognition in audio, visual and text data. Through context-inference, context-awareness may be achieved.

Context-inference is the process of detecting or inferring the context from input data sources (data providers or sensors) and is the primary feature for achieving context-awareness. This process can be fairly sophisticated, incorporating methods and techniques that range from

simple statistical operators to complex machine learning algorithms (Huynh and Schiele, 2005).

Context-awareness manages information entities known as contexts. A system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task (Dey and Abowd, 1999).

One important functionality provided by a context-aware infrastructure is context interpretation to derive high-level contexts. In context-aware systems, high-level contexts augment context-aware applications by providing summary descriptions about users' states and surroundings. They are generally inferred from low-level, explicit contexts which are directly provided by hardware sensors and software programs (Tan, Zhang, Wang and Cheng, 2005).

Context can help create a baseline for behavior (Wodarski and Hopson, 2011), therefore. Such a behavioral baseline may be utilized to control system behavior, its responses – to prevent a system from getting enticed and drawn out into a position that will even allow exposition of its vulnerabilities. A behaviour based and behavior-bound system may permit only acceptable behavior, while closing the route to all other undesirable behavior, i.e. to malbehavior. From that perspective, a re-look at Figure 2 reveals how symptoms of malbehavior manifest themselves. It is proposed here, that focusing on preventing malbehavior may be more rewarding than having a zillion products each to treat one symptom.

Therefore, keeping out malbehavior is going to be extremely important for mankind to progress to secure Ubiquitous computing. Cafezeiro (2008) asserts: in particular, context-awareness, i.e. the ability of applications to detect changes in their environment and to adapt their behavior, accordingly, has become the paramount programming paradigm for Ubiquitous computing systems.

A context-aware security solution can protect from both insiders and outsiders (Litan, 2014), though most security products are only beginning to utilize this concept. Many approaches to security now factor context-awareness, including with IOT devices (Trnka, Tomasek & Cerny, 2017). The following proposed Contextual framework is the first ever most comprehensive framework, that may form the core of efforts to understand and prevent malbehavior, for any context-aware security system:

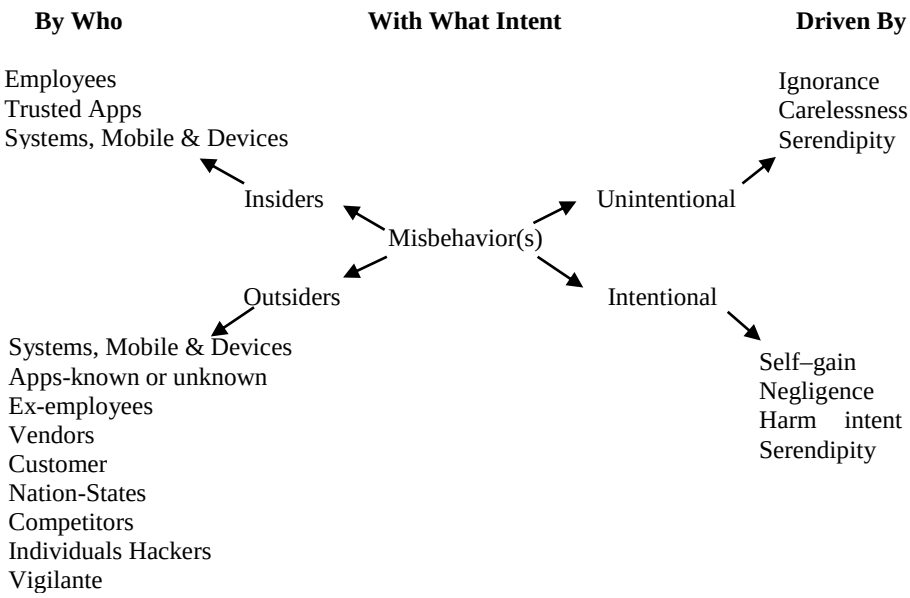

Fig-2 Contextual Framework for Malbehavior

After fully understanding the actors (insider, outsiders), their intent and the reasons for it, security use cases need to be as detailed as possible to block malbehavior. This framework may also make it easy to co-relate to suspects, when indeed there is a problem. The purpose of every Cyber-attack is to cause some enduring damage, even if briefly. Resilience is exactly what brings back an attacked system to normalcy. In the context of security, the Department of Homeland Security (U.S.A.) defines the term resilience as: the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies (DHS, 2010).

Highly resilient systems offer a dis-incentive for attacks. Few attackers choose a target they know is unlikely to be significantly impacted, or for long enough for them to get business done. It is for this reason the United States officially recognized resilience as a cornerstone of the national security doctrine in the 2010 National Security Strategy document. Further, taking into cognizance the inseparableness of the Cyber and Physical worlds, for the sake of integrated Cyber-Physical world security, the Presidential Policy Directive calls upon the state to: "Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time" (Presidential Policy Directive, 2013).

Strictly, within the context of computing and networks that may survive despite malicious attacks, research has established that context-awareness driven resilience is a key enabler. A key factor in the reliability and security of network infrastructure is its resilience in the face of denial of service attacks (Andre, Smith and Troncon, 2009).

RFC 5452 talks about specific actions to be taken for making DNS more resilient. Researchers at Kansas University (Kansas University Resilinets Project, 2008) have declared context-awareness is an enabler of resilience in sustainable networks, that may survive despite malicious attacks.

Context and context-awareness can be used differently for security. Fireeye, created by the CIA, provides a staging environment between all outside traffic and actual servers. The staging environment provides an effective context in which malbehavior gets to act and therefore gets detected before malbehavior reaches actual servers (Davis, 2014).

The ability to be context-aware will also be key for the upcoming area that utilizes brain waves-based computing, i.e. BCI: Brain-Computer Interfacing (Faller, 2012), which is expected to be the norm in the era of Ubiquitous Computing. Also, so far most of the attacked, ignored the "who attacked from where" part. However, of late, Blackhat security training has begun to advocate the F3EAD methodology used by US Special Operations Forces (Blackhat Asia Training, 2015) for counter-terrorism. The Contextual framework below advances the concept of information security towards sustainability, by including broader requirements.

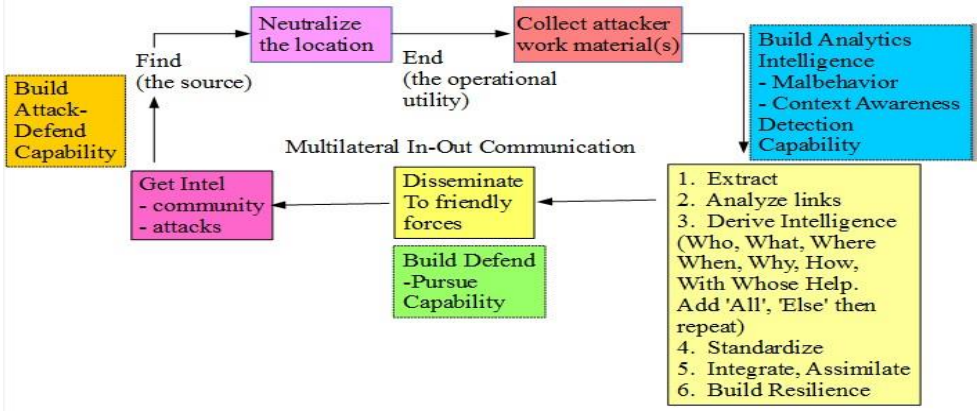

Fig-3 Framework for Integrated Cyber-Physical Sustainable Information Security

Taking into cognizance the fact that security in the Cyber and Physical world are connected, the above framework advocates pursuing malbehavior actors in the physical world- to find them, to neutralize their harmful capabilities, to collect intelligence and infiltrate their links and networks, to communicate that information to partners (friendly forces) in order to continue to neutralize all such, paving the way for a global and united fight against malbehavior, so that sustainable information security can follow.

In the connected technology enabled Big Data world that is emerging, it must be also emphasized that inter-state (nation) communication and relationships need to play their important roles – so that internet rules are the same for everyone, so that internet crime can be successfully prosecuted anywhere in the world, so that the internet can be safer and be secured.

Notably, the Presidential Policy Directive also talks about the development of a vendor neutral security framework and emphasizes, among other aspects, on open communication and co-ordination between various actors – public as well as private (Presidential Policy Directive, 2013), both in-state and out-of- state. Legislative issues are important to security, as has also been observed by Chaudhary, Ibrahim and Bashir (2017).

5. Big Data can Aid Development of Context

Given the challenges discussed so far, development of capabilities for a broad context (Jess, 2014) are necessary.

One of the approaches in building information security context can be via utilization of metadata. As per the McKinsey Global Institute (MGI) research (James et al, 2014), creating substantial new value from Big Data does not necessarily require jumping directly to complex analytical big data levers. MGI recommends techniques to "scrub" the data to remove errors and ensure data quality, to place data into standard forms, so that metadata can be added to describe the data being collected.

The documentation and description of datasets with metadata (James et al., 2014)—data about data— enhances the discoverability and usability of data both for current and future applications, as well as forming a platform for the vital function of tracking data provenance.

Master data can come to rescue and help in building context for delivering customer-centric outcomes. With Master Data Management

(MDM), organizations can correlate unstructured text to existing master records, discover linkages between text and relevant master entities, and enrich the master record with additional information. It is established beyond doubt that master data and Big Data complement and enrich each other: master data helps create the context for Big Data, while Big Data creates content for master data management (IBM White Paper, 2014).

Metadata (Prevosto and Marotta, 2013) and metadata management (Dumbill, 2013) become even more important when dealing with large, complex, and often multi-sourced data sets.

A survey has revealed that Big Data scientists are expecting to have to work with at least the following sources of data (Olavsrud, 2014):

1. Time-series data
2. Business transactions
3. Geospatial / location data
4. Networks
5. Clickstream data
6. Health Records data
7. Sensor data
8. Image data
9. Genome data.

Scientists will have to be prepared to create information security context models that may be able to utilize input from the above data types.

Finally, we conclude Big Data Analytics may be able to deliver sustainable information security through what are popularly known as the 6Cs of Big Data (Russom, 2013):

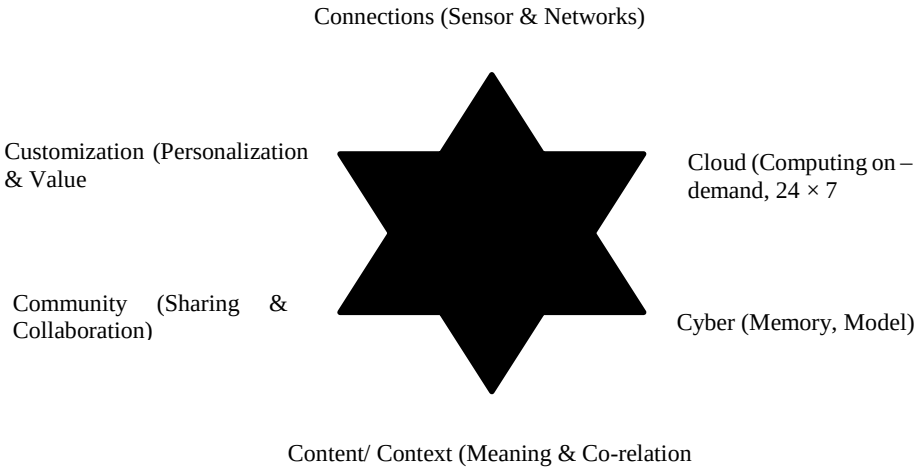

Fig-4 The 6 C's of Big Data

Raw big data may be available from various sensors and networks. These sensor logs and raw data may be stored in the cloud, for anytime on-demand analytics. Several models and algorithms may also be stored on servers and be run to understand which one provides the best analysis. Using metadata and other content, patterns spanning nations, misbehavior, intelligence and actors may emerge to yield contexts - contexts that may be clarified by augmenting inputs from the Cyber-Physical continuum and then be created for co-relations to be drawn. Useful nuggets of information so drawn after analytics may be quickly disseminated for mass or specific consumption, visualizations of which may be fine-tuned for the requirements through available customization.

It is therefore clear that Big Data can help create an encompassing canvas for sustainable information security.

6. Major Findings

This research establishes the fact that the concept of information security is rather silently undergoing a metamorphosis. Most existing paradigms of information security are already sunset, making way for machines and Big Data analytics based, context-awareness driven security. Piecemeal approaches will have to give way to an integrated malbehavior prevention approach, not only in the Cyber world, but also in the Physical world – since sustainable information security can no longer be afforded to be secondary to National security.

It is only now that waves of adoption of PCs, mobiles, devices, IOT have started yielding Big Data with hidden "gems of wisdom" - information that can be very precious and may help form the overall context within which certain security events may have happened. However, the role of all these together: Machine Learning, Context Aware Computing, Big Data Analytics and Metadata in the domain of information security - has hardly been well explored.

While it is generally agreed that Big Data can help improve information security, context-awareness may be generated through Big Data to enable machines to disallow malbehavior. The Cyber-Physical continuum model cohesively seeks to address sustainable information security issues. This research seeks a paradigm shift in the way information security has been looked at, while proposing:

1. a first-time contemporary picture of the information security context, which makes it clear why current approaches are, at best, piece-meal
2. a contextual framework on malbehavior – that may be expected to form the core of context- awareness based security approaches, and
3. a contextual framework for integrated Cyber-Physical Information Security – that may have a chance of delivering sustainable information security, so necessary in the Ubiquitous computing era towards which the world is speedily and inevitably headed.

7. Methodology

This work draws from academic literature research, from industry surveys conducted by a diverse set of industry leaders, from the experiences of industry leaders and from practices adopted by those carrying out Big Data analytics in information security area and other areas of analytics.

8. Conclusion

Information security issues arise from malbehavior – of the system, voluntarily or otherwise. A network or a computer by themselves have neither vulnerabilities, nor strengths – usually, it is human minds, behaviors and contexts that decipher the environment in which to deploy tactics to turn something benign to hostile for a position of relative advantage. This paper therefore concludes that the machine-enabled Big Data created context-awareness based malbehavior prevention centric approach recommended herein, for sustainable Cyber-Physical information security, is key to formation of a new paradigm in information security.

9. Limitations

As is evident from the Big Picture – Context for information security, the problem has too many failure points despite significant efforts being made to address its different facets, yet few concerted and integrated efforts have yielded results for curing the overall disease.

To capture the entire landscape, this work, therefore occasionally had to be limited to solutioning from the proverbial 10,000 feet view.

While the malbehavior approach may form the core of context-aware security systems, the capabilities delivered through sensors and Big Data analytics are crucial dependencies. Even after all is given, developing context is a tremendous challenge and context-aware systems are yet to

deliver a critical function such as security, on a large scale, though context-awareness has shown and proven promise in non-critical applications.

The war for Cyber-security is on, but there still are sides to choose, from. Till an integrated non- discriminatory effort is made to remove the disconnect between Cyber and Physical security worlds, no information security is going to be sustainable. It is encouraging, though, to see some nations take a lead in this direction, calling for collaboration and co-operation for a happy ubiquitous future.

References

1. Adrian, M. (2011), "Information Management Goes 'Extreme': The Biggest Challenges for 21st Century CIOs," *Gartner Publications*, At: http://www.sas.com/offices/NA/canada/lp/Big- Data/Extreme Information Management.pdf, Accessed on: 2014/07/24
2. Andre, P.S., Smith, K., Troncon, R. (2009), "XEP-0205: Best Practices to Discourage Denial of Service Attacks," *Extensible Messaging and Presence Protocol (XMPP)*, At: http://xmpp.org/extensions/xep-0205.html, Accessed on: 2015/07/01
3. Belsky, G. (2012), "Why Text Mining May Be The Next Big Thing," *Time Magazine Cover Article*, At: http://business.time.com-/2012/03/20/why-text-mining-may-be-the next big-thing/ , Accessed on: 2014/05/29
4. Bilton, N. (2013), "Adobe Breach Inadvertently Tied to Other Accounts," *The New York Times*, At: Codenomicon (2014), "Heartbleed," *Codenomicon, Inc.*, At: http://heartbleed.com/, Accessed on: 2015/01/05
5. Blackhat Asia Training (2015), "Intelligence Driven Security," *Blackhat (Hackers) Security Training*, At: https://www.blackhat.com/asia-15/training/intelligence-driven-security.html, Accessed on: 2015/01/15
6. Blackhat Briefings (2013), "Defending Networks with Incomplete Information – A Machine Learning Approach," *Blackhat (Hackers) Security Forum*, At: https://media.blackhat.com/us- 13/US-13-Pinto-Defending-Networks with Incomplete Information A Machine Learning-Approach-WP.pdf, Accessed on: 2015/01/31
7. Booz Allen & Hamilton, EMC(2013), "Big Data Fuels Intelligence Driven Security-IO," *EMC*, At:http://www.emc.com/collateral/industry-overview/big-data-fuels-intelligence-driven- security-io.pdf, Accessed on: 2015/01/12

8. Cafezeiro, I. et al. (2008), "A Formal Framework for Modeling Context-Aware Behavior in Ubiquitous Computing", *Leveraging Applications of Formal Methods, Verification and Validation - Communications in Computer and Information Science Volume 17, 2008, pp 519- 533*
9. CFP CASCCIT(2018): On Context-Aware Security in Cloud Computing and Internet of Things 2018, http://wikicfp.com/cfp/servlet-/event.showcfp?eventid=73533, Accessed on: 2018/03/01
10. Chaudhry, J., Ibrahim, A. and Bashir, A.K. (2017), "Internet of Threats and Context Aware Security: Part One", in IEEE Future Directions, At: http://sites.ieee.org/futuredirections/tech-policy-ethics/january 2017/internet of threats and-context-aware-security-art-one/,Accessed on: 2018/12/08
11. Codenomicon (2014), "Heartbleed," *Codenomicon, Inc.*, At: http://heartbleed.com/, Accessed on: 2015/01/05
12. Ollett, S. (2014), "Five New Threats to Your Mobile Device Security," *Chief Security Officer Online (CSOOnline)*, At: http://www.cs-oonline.com/article/2157785/data-protection/five-new- threats-to-your-mobile-device-security.html, Accessed on: 2015/01/13
13. Damballa (2014), "State of Infections Report," *DamballaInc.*,At:https://www.damballa.com/downloads/r_pubs/Damballa_Q114_State_of_Infections_Report.pdf, Accessed on: 2015/01/25
14. Davis, S. (2014), "Target Ignored Systems Hacking Warnings Report," *CBS News*, At: http://www.cbsnews.com/news/target-ignored-systems-hacking-warnings-report-says/, Accessed on: 2015/01/11
15. Deloitte (2017), "Security Awareness - People and Technology", Deloitte consulting, At: https://www2.deloitte.com/content-/dam/Deloitte/-cy/Documents/risk/crs/CY_Risk_Security Awareness Services Flyer_Noexp.pdf, Accessed on: 2019/01/22
16. Dey, A. K. and Abowd, G. D.(1999), "Towards a Better Understanding of Context and Context- Awareness," *HUC'99 Proceedings of the 1st International Symposium on Handheld and Ubiquitous Computing, pp 304-307* At: https://smartech gatech.edu/bitstream/handle/-1853/3389-/9922.pdf;jsessionid=45FA2C938FC50B4A7867F28318BB7462.smart 1?sequence=1,Accessed on: 2015/01/22
17. DHS (2010), "Resilience," *Department of Homeland Security (DHS)*, At: http://www.dhs.gov/topic/resilience, Accessed on: 2015/01/18

18. Dilanian, K. (2013), "Cyber-attacks a Bigger Threat Than Al Qaeda, Officials say," *Los Angeles Times*, At: http://articles.latimes-.com/2013/mar/12/world/la-fg-worldwide threats-20130313, Accessed On: 2015/01/31
19. Dumbill, Edd (2013), "Big Data Variety Means That Metadata Matters," *Data Driven- Forbes Magazine*, At: http://www.forbes com/sites/edd-dumbill/2013/12/31/big-data-variety-means- that-meta-data matters/, Accessed on: 2014/08/08
20. Faller, J. et al. (2012), "Prototype of an Auto-Calibrating, Context-aware, Hybrid Brain- Computer Interface," *Proceedings of the Engineering in Medicine and Biology Society (EMBC), 2012 Annual International Conference of the IEEE, pages 1827-1830* At:http://ieeexplore-.ieee.org/xpl/freeabs_all.jsp?arnumber=6346306&abstractAccess=yes& userTy pe=inst, Accessed on: 2015/01/06
21. Fung, K. (2014), "Google Flu Trends' Failure Shows Good Data > Big Data," *Harvard Business Review Blog Network*, At: https://hbr.org/2014-/03/google-flu-trends-failure-shows-good-data- big-data/, Accessed on: 2015/08/01
22. Gartner (2014), "The Impact of the Internet of Things on Data Centers," *Gartner*, At: http://www.gartner.com/newsroom/id/2684616, Accessed on: 2015/01/16
23. Grimes, S. (2013), "Big Data: Avoid 'Wanna V' Confusion,"*Information Week*, At: http://www.informationweek.com/big-data/big-data-analytics/big-data-avoid-wanna-v- confusion/d/d-id/1111077?, Access-ed on: 2014/08/31
24. Harford, T. (2014), "Big Data: Are We Making a Big Mistake?" *The Financial Times*, At: http://www.ft.com/cms/s/2/21a6e7d8-b479-11e3-a09a-00144feabdc0.html, Accessed on: 2014/07/29
25. Hobbs, J. R., Walker, D. E. and Amsler, R. A. (1982), "Natural Language Access to Structured Text," *Proceedings of the 9th conference on Computational linguistics 1. pp. 127–32*
26. Hubert, A. and van Mook, R. (2009), "Measures for Making DNS More Resilient Against Forged Answers," *International Engineering Task Force (IETF)*, At: https://tools.ietf.org/html/rfc5452, Accessed on: 2015/01/08
27. Huynh, T. and Schiele, B. (2005), "Analyzing Features for Activity Recognition," *In Proc. of the 2005 joint conference on Smart objects and ambient intelligence (sOc-EUSAI '05) , pages 159–163, New York, NY, USA, 2005, ACM*

28. IBM (2007), "Internet Security Services," *IBM*, At: http://www.ibm.-com/jm/download/IBM_ISS_Overview.pdf, Accessed On: 2015/01/13
29. IBM White Paper (2014), "The MDM Advantage- Creating Insights From Big Data," *IBM Research*, article number: IMM14124-USEN-01, At: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=BK-&infotype=PM&appname=SWGE_IM_EZ_USEN&htmlfid=IMM14124USEN&attachment=IMM14124USEN.PDF&ce=ISM0056&ct=swg&cmp=ibmsocial&cm=h&cr=crossbrand&ccy=us#loaded , Accessed on: 2014/08/03
30. Trnka, M., Tomasek, M., Cerny,T. (2017), "Context-Aware Security Using Internet of Things Devices", ICISA 2017- the International Conference on Internet Security and Applications, Information Science and Applicationspp 706-713, At: https://link.springer.com/-chapter/10.-1007%2F978-981-10-4154-9_81, Accessed on: 2018/12/22
31. Inmon, B. (2013), "Data, Metadata and Big Data," *B-eye-network*, At: http://www.b-eye- network.com/view/16943 , Accessed on: 2014/05/29
32. K.N.C. (2014), "The Backlash Against Big Data," *The Economist Explains*, At: http://www.economist.com/blogs/-economistexplains/2014/04/economist-explains-10?zid=316&ah=2-f6fb672faf113fdd-3b11cd1b1bf8a77, Accessed on: 2014/06/25
33. Kansas University Resilinets Project (2008), "Resilinets Principles," *Kansas University Resilinets Wiki*, At: https://wiki.ittc.ku-.edu/resilinets/File:Resilinets-principles.png, Accessed on: 2015/01/17
34. Kaplan, R. and Kaplan, D. (2014) "USB is Now UEC – Use with Extreme Caution," *Chief Security Officer Online (CSOOnline)*, At: http://www.csoonline.com/article/2836299/data- protection/usb-is-now-uec-use-with-extreme-caution.html#tk.ifw_nsdr_ndxprmomod, Accessed on: 2014/12/28
35. Kar, Saroj (2014), "Garner Reports: Big Data Will Revolutionize the Cybersecurity in Next Two Years", *CloudTimes*, At: http://cloudtimes.org/2014/02/12/gartner-report-big-data-will-revolutionize-the-cybersecurity-in-next-two-year/, Accessed on: 2015/01/19
36. Kovacs, E. (2015) "Researchers Bypass All Windows Protections by Modifying a Single Bit", *The Security Week*, At: http://www.securityweek.com/researchers-bypass-all-windows- protections modifying single bit, Accessed on: 2015/02/11

37. Lampe, J. (2014), "Three Security Practices that IOT Will Disrupt," *Chief Security Officer Online (CSOOnline)*, At: http://www.csoonline.com/article/2599509/data-protection/three- security-practices-that-iot-will-disrupt.html, Accessed on: 2015/01/08
38. Lazer, D., Kennedy, R., King, G. and Vespignani, A. (2014), "The Parable of Google Flu: Traps in Big Data Analysis," *Science Vol. 343*, At: http://www.uvm.edu/~cmplxsys/wp- content/uploads/lazer-flu-science-2014.pdf, Accessed on: 2014/08/09
39. Litan, A. (2014), "Avivah Litan on 'Context-Aware' Security", At: https://www.bankinfosecurity.com/interviews/litan-at-summit-i-2317, Accessed on: 2015/01/01
40. Leuuw, K.D. (2007), "The History of Information Security", Elsevier Publishing https://doi.org/10.1016/B978-0-444-51608-4.X5000-7, Accessed on: 2019/01/22
41. Manyika, J. et al. (2014), "Big data: The Next Frontier for Innovation, Competition, and Productivity," *McKinsey Global Institute Report, p1-22*, At: http://www.mckinsey.com/insights/business_technology/big_-data_the_next_frontier_for_innova tion Accessed on: 2014/08/01
42. Marcus, G. and Davisparil, E. (2014), "Eight (No, Nine!) Problems With Big Data," *The New York Times*, At: http://www.nytimes.com/2014/04/07/opinion/eight-no-nine-problems-with big data.html, Accessed on: 2014/07/21
43. McCrory, Anne (2000), "Ubiquitous? Pervasive? Sorry They Don't Compute," *The Computer World*, At: http://www.computerworld.com/article/2593079/ubiquitous—pervasive--sorry--they- don-t-compute.html, Accessed on: 2014/12/31
44. Moore, M. (2014), "China Builds Computer Network Impenetrable to Hackers," *The Telegraph*, At: http://www.telegraph.co.uk/news/worldnews/asia/china/11216766/China-builds- computer-network-impenetrable to hackers.html , Accessed on: 2014/09/09
45. National Center for Text Mining (2013), *NaCTeM*, At: http://www.nactem.ac.uk, Accessed on: 2015/01/09
46. Neill, J. (2014) "Big Data Needs Big Context," *Harvard Business Review Insight Center Report From Data To Action (AST0127658), Harvard Business Publishing, page(s) 32-33*
47. Nichols, S. J. V. (2015), "The Year The Internet Crashes," *Computer World*, At: http://www.computerworld.com/article/2866064/2015-the-year-the-internet-crashes-hard.html, Accessed on: 2015/02/11
48. Olavsrud, T. (2014), "Data Scientists Frustrated by Data Variety Find Hadoop Limiting," *Chief Information Officer (CIO)*, At:

http://www.cio.com/article/2449814/big-data/data-scientists- frustrated-by-data-variety-find-hadoop-limiting.html Accessed on: 2015/01/28

49. Oxford Dictionary (2015),*Oxford Dictionaries*, At: http://www.oxford-dictionaries.com/definition/english/context, Accessed on: 2015/01/21
50. Perlroth, N. (2013a), "Chinese Hackers Infiltrate New York Times Computers," *The New York Times*, At: http://www.-nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0, Accessed on: 2015/01/24
51. Perlroth, N. (2013b), "Antivirus Makers Work on Software to Catch Malware More Effectively,"*TheNewYorkTimes*,At: http://www.ny-times.com/2013/01/01/technology/antivirus-makers-work-on-software to catch- malware-more-effectively.html?pagewanted=-all&_r=0, Accessed on: 2015/01/04
52. Phneah, E. (2012), "Mobile apps pose biggest threat," *ZDNet*, At: http://www.zdnet.com/article/mobile-apps-pose-biggest-threat/, Accessed on:2015/01/05
53. Ponemon, L. (2013), "First Ponemon Study on Big Data Analytics in Cyber Defense is a National Wake Up Call," *Teradata, Inc.*, At: http://in.teradata.com/cybersecuritythreat/?LangType=16393&LangSelect=true#tabbable=0&tab1=0&tab2=0&tab3=0&tab4=0, Accessed on: 2015/01/02
54. Presidential Policy Directive (2013), "Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience," *Department of Homeland Security (DHS)*, At: http://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf, Accessed on: 2015/01/08
55. Press, G. (2014), "6 Predictions For The 125 Billion Big Data Analytics Market in 2015," *Forbes*, At: http://www.forbes.com-/sites/gilp-ress/2014/12/11/6 predictions forthe 125billion big dataanalytics market in 2015/ Accessed on: 2015/01/31
56. Prevosto, V. and Marotta, P. (2013), "Does Big Data Need Bigger Data Quality and Data Management?"*VeriskAnalytics,Inc.*,At: http:-//www.redbooks.ibm.com/redpapers/pdfs/redp5070.pdf, Accessed on: 2014/08/02
57. Prince, B. (2015), "Employees Not Following Policy Biggest Threat Endpoint Security IT Pros Say," *The Security Week*, At: http://www.securityweek.com/employees-not-following-policy-

biggest-threat-endpoint-security-it-pros-say, Accessed on: 2015/02/11

58. Rieck, K. (2011), "Computer Security and Machine Learning: Worst Enemies or Best Friends?" *Proceedings of SysSec Workshop (SysSec), 2011 First, IEEE*, At: http://ieeexplore.ieee.org-/xpl/articleDetails.-jsp?reload=true&arnumber=6092778, Accessed on: 2015/01/20
59. Rieck, K., Trinius, P. , Willems, C. , and Holz, T. (2011), "Automatic analysis of malware behavior using machine learning," *Journal of ComputerSecurity*,At:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.335.8246&rep=rep1&type=pdf, Accessed on: 2015/01/26
60. RP, Srikanth (2013), "Security Analysis Set Transform Security Landscape," *The Information Week*, At: http://www.in-formationweek.in/informationweek/news-analysis/179190/security-analytics-set-transform-security-landscape, Accessed on: 2015/01/02
61. Russom, P. (2013), "Real Time Business Analytics from Big Data," *Splunk, Inc.*, At: http://www.splunk.com/web_assets/pdfs/secure/Real-time_Business_Analytics_from_Big_Data.pdf Accessed On: January 25, 2015
62. Samson, T. (2013), "9 Top Threats To Cloud Computing Security," *InfoWorld*, At: http://www.infoworld.com/article/2613560/cloud-security/9-top-threats-to-cloud-computing- security.html, Accessed on: 2015/01/12
63. Santos, A. C. et al. (2010), "Challenges in the Development of Context-Inference Systems for Mobile Applications," *Proceedings of International Workshop on Programming Methods for Mobile and Pervasive Systems (PMMPS), colocated with Pervasive (2010)*, At:http://web.ist.utl.pt/diogo.ferreira/papers/santos10challenges.pdf, Accessed on: 2015/01/13
64. SAS Institute (2013), "Five Big Data Challenges," *SAS Institute, Article number 106263_S106008.031*, At: http://www.sas.com/resou-rces/ass-et/five-big-data-challenges- article.pdf, Accessed on: 2014/08/02
65. Tan, J. G., Zhang, D., Wang, X. and Cheng, H. S. (2005), "Enhancing Semantic Spaces with Event-Driven Context Interpretation," *In Proceedings of the Third international conference on Pervasive Computing (PERVASIVE'05), Hans-W. Gellersen, Roy Want, and Albrecht Schmidt (Eds.). Springer-Verlag, Berlin, Heidelberg, 80-97*
66. Teller,T.(2012),"TheBiggestCybersecurityThreatsof2013,"*Forbes*,At: http://www.forbes.com/sites/ciocentral/2012/12/05/the-biggest-cybersecurity-threats-of-2013- 2/, Accessed on: 2015/01/18

67. Thibodeau, P. (2015),"More Than 1 Billion Records Breached in 2014," *Computer World*, At: http://www.computerworld.com-/article/28-82708/more-than-1b-records-breached-in-2014.html?phint=newt%3Dcomputerworld_security&phint=idg_eid%3D65c9407581c5e91e1bc007c68025f7b8#tk.CTWNLE_nlt_security_2015-02-13, Accessed on: 2015/02/11
68. Toussaint, G. T. (1978), "The Use of Context In Pattern Recognition", *Pattern Recognition Vol.10 pp. 189-204.*,At: http://www-cgrl.cs.mcgill.ca/~godfried/teaching/mir-reading-ssignments/Context-in-Pattern-Recognition.pdf Accessed on: January 18, 2015
69. Vijaiyan, J. (2015), "6 Ways The Internet of Things Will Transform Enterprise Security," *Chief Security Officer Online (CSOOnline)*, At: http://www.csoonline.com/article/2140007/security/6- ways-the-in-ternet-of things will-transform-enterprise-security.html, Accessed on: 2015/01/15
70. Witten, I.H. (2005), "Text mining," *Practical Handbook of Internet Computing, edited by M.P. Singh, pp. 14-1 - 14-22. Chapman & Hall/CRC Press, Boca Raton, Florida*
71. Wodarski, J. S. and Hopson, L. M. (2011), "Research Methods for Evidence-Based Practice,"*Sage Publications Chap.5 Pg 73 Oct. 2011*