# INSTITUTE FOR DEVELOPMENT AND RESEARCH IN BANKING TECHNOLOGY

**(Established by Reserve Bank of India)**

## FIFTH IEEE INTERNATIONAL CONFERENCE ON IDENTITY, SECURITY AND BEHAVIOURAL ANALYSIS (ISBA)

January 22-24, 2019

## *INAUGURAL ADDRESS*

Basic Research, as we all know, refers to the study that is aimed at expanding the existing base of scientific knowledge, whereas Applied Research is the research that is designed to solve specific practical problems or answer certain questions. While the former focuses on developing scientific knowledge and predictions, the later focuses on development of technology and technique. While universities and academia concentrate their efforts on basic research, applied research is generally carried out by the research institutions specifically set up by commercial entities or funded by them. These institutions connect the academia and the user community. IDRBT is at this intersection of academia and the banking industry. It has several platforms in which it facilitates meeting of the minds of all stakeholders like the academia, technology companies, the banking and financial institutions, the regulators and other public policy authorities. IDRBT's sponsoring the ISBA 2019 Conference on these three days is a part of its such role. I am very happy to be inaugurating

this Fifth IEEE International Conference on Identity, Security and Behavioural Analysis.

**Security**

Security is fundamental to banking. The very origin of banking as a vocation started in 1600s from the comfort of the people who entrusted their money with the banker in the secured knowledge that it is safe and will be available when asked for. That security permeates even today in every type of operation of the banks and financial institutions. At every stage of development, and on launching of every new financial product or service, the banker has to continuously extend the assurance that the public money entrusted with him is safe and secure. More importantly, when banking enhances the technology and attempts to use cutting edge technology, the assurance related to safety and security of funds that is needed is of very high order. Given the abstract character of the digital technology, the enormity of volume of digital transactions, the speed with which the digital transactions are carried out – many times transcending geographical borders, continuous demand on improving digital security has been persistently seen. Added to this is the ever present threat dimension of fraudsters trying to take advantage of loopholes in security, challenging the security edifice that has been assiduously built, posing grave risk to the confidence that people have in digital banking. Naturally, the concept of information security providing assurance on confidentiality, integrity and availability of information

has evolved into cyber security that will in addition assure security of data storage locations, the technologies used to access information, the information highway and its various aides. Hence it is no wonder that cyber security has emerged as a separate discipline within the information technology research.

The banking and financial sector is experiencing cyber risks more because of the increased use of rapidly evolving, sophisticated, and complex technologies, wide use of third-party vendors, increased use of mobile technologies by customers, including the rapid growth of the Internet of Things and the heightened cross-border information security threats.

A new dimension of cyber security threat has been the perceived and real threat of state sponsored attacks on a nation's vital and critical systems. It is widely believed that future wars between nations will be based on cyber-attacks and in cyber space. Protection of such critical systems of an economy like the defence, power, transport, energy and financial systems has assumed urgent and significant attention.

The current research attention has been on securing digital assets, better smart IoT botnets, protecting critical national infrastructure, Crypto jacking, Ransomware, Advanced Persistent Threat(APT) groups, State Sponsored attacks, Encrypted traffic malware, AI assisted malware etc. I am glad that IDRBT and ISBA have specific focus in these areas.

**Identity**

Banking and finance deal with millions of customers and thousands of staff. Identifying uniquely each of these individuals is very critical for these institutions, especially when these persons will operate through digital means. It enhances its security. Thus identity is a part of security only. However, technological developments in this sphere over the years have been evolving into a special discipline. When establishing identity of parties evolved through what the 'users know' to what the 'users have' to what the 'users are', attention has turned towards Biometrics – like the finger prints, iris, face, voice, gait and the like and with its overtones on biological and physical aspects, identity has now become a separate discipline.

**Behavioural Analysis**

Despite the developments in security and identity related instruments, procedures and operations, any number of problems have been encountered by banks and financial institutions. These problems led to compromising security and integrity of information and money. Ignorant and gullible users are being compromised, in spite of use of biometric based identity and secured transaction protocols. While the banks and the financial institutions could protect themselves legally by following the best in trade security and identity procedures, when such compromises arose, they do feel moral responsibility towards protection their own users from such malpractices. Even regulators are also increasingly demanding greater

consumer protection standards. More importantly, early identification of misuse and limiting damage have attained critical importance.

Another development that compels higher thrust on Behaviour Analysis is the internationally coordinated measures for preventing formal financial system being a conduit for money laundering, drug trafficking and financing terrorism. The grave responsibilities cast on the banks and financial institutions, the exemplary penalties for every failure in this regard and the magnitude of the damage to their reputation have all generated urgency for solutions based on behavioural analysis for raising early warning red signals to identify and prevent these high profile international crimes related financial transactions.

With the developments in big data analysis, behavioural analysis has taken centre stage. Initially, in early 2000s, such an analysis was used for predicting customer buying patterns. Later, its potentials for enhancing User and Entity Behaviour identity have been recognised. In 2015, Gartner published a market guide for what it coined as user and entity behaviour analytics (UEBA). This is a maturing technology. Business Analytical tools have advanced profiling capabilities. Big data analytics and Machine learning algorithms and statistical analysis are used. Currently the use cases include identifying Privileged account misuse, Compromised account detection, Compromised machine/system detection, Insider Threat detection, Detection of

Data Theft, Incident prioritisation, Application monitoring and Cloud Security Monitoring.

**Security and Privacy**

The hot subject that has received wider attention in recent times and debate is data security and data privacy. You will all recall that in August 2017, a nine-judge bench of the Supreme Court declared privacy as a fundamental right of Indian citizens. The Court ruled that the right to privacy is protected by the Constitution as an intrinsic part of the right to life and personal liberty under Article 21. The Court also observed that 'informational privacy', or the privacy of personal data and facts, is an essential facet of the right to privacy.

This is the case not just in India, but over the whole world. The EU General Data Protection Regulation (GDPR) is the most talked about law. The regulation has fundamentally reshaped the way in which data is handled across every sector, including banking and beyond. In India, Justice Shrikrishna Committee recommendations on data privacy protection and the consequent Personal Data Protection Bill 2018 are the relevant developments.

In my view, we need to understand two facets of this data privacy – one is that data privacy in a commercial context and the other is in a democratic and human rights context. The general understanding and approach to these two aspects in various jurisdictions are as follows: The general trend is that data privacy is a fundamental right of the individuals and any unconsented use thereof by entities would result

in heavy penalties. Further, even government and public policy authorities are also being bound by these regulations.

In the commercial context, primacy has been accorded to informed consent by the individual. Unless one has given explicit consent, his/her personal data cannot be shared or processed. Further, any person processing personal data of individuals is obligated to do so in a fair and reasonable manner. In other words, personal data should be processed only for the purposes it was intended for in the first place. The key aspects here are, just to repeat, informed consent, and checks and balances on the commercial entity, including heavy penalty for violations.

In the context of human right and democratic overtones, the trends in data privacy have impacted or likely to impact governmental and public policy authorities in significant and powerful ways. Here, informed consent is not considered to be sufficient. For example, the Justice Srikrishna Committee Report had argued that the validity of consent given by the individual while availing State welfare benefits is questionable, given the imbalance of power between the citizen and the State. Further, the Report states that only those government bodies which are performing functions directly related to the provision of welfare benefits or regulatory functions should be allowed non-consensual processing of data. The Report acknowledges that non-consensual processing by government entities for all kinds of public functions may be too wide an exception to consent.

The Supreme Court, in Puttaswamy vs UoI, allowed exceptions to the right to privacy of an individual under certain situations. These include cases where a larger public purpose is satisfied by the infringement of privacy of an individual. Such an exemption must be backed by a law, and must be necessary for and proportionate to achieving the purpose. The requirements of necessity and proportionality are very important. We should remember that the Supreme Court, in deciding the constitutionality of Aadhaar, had declared the provision to link Aadhaar numbers with SIM cards or for opening bank accounts as disproportionate, and thereby unconstitutional.

Why these debates are relevant to this Conference of scientists? This Conference is about Identity, Security and Behavioural Analysis and all these three concepts now are acquiring legal implications. It is relevant to recognise that the law of countries define 'personal data' as any information which renders an individual identifiable, and 'sensitive personal data' is defined to include passwords, financial data, biometric and genetic data, caste, religious or political beliefs and data 'processing' is defined as any operation, including collection, manipulation, sharing or storage of data. While basic research has the freedom not to worry about the constraints of any sort, including legal constraints, applied research will have to fully factor in the prevalent legal framework and also evolving framework.

Following the Supreme Court order in the Aadhaar case, there is great uncertainty, confusion and reluctance on the part of banks and

financial institutions to use biometrics as the basis for identifying individuals. Several fintech companies have to redraft their business models because of this. Their cost of operations have tremendously increased consequently, affecting their profitability and also threatening their continued existence. Banks and financial institutions who have outsourced processing of their data are now a worried lot because of the proposed ban on cross-border transfer of sensitive data which is proposed to include even passwords and financial data; they, more specifically the payment sector entities, are concerned about the data localisation requirements.

Thus we can discern a palpable need for technical solutions for all these problems. Applied research's exact role is that only. Hence, I would like to exhort this Conference and the participants here, to pay special focus on these burning questions and find viable solutions that would be within the legal compliance framework.

One idea that I will request some of you to pursue is to find a solution for the problem of storage and access of biometric data. Technology has earlier found a solution for the security of data through the concept of Public Key Infrastructure(PKI) by splitting the key into its public and private parts. Similarly, is it possible to split 'biometric data' into two parts, one the public part to be with the government, and for that matter with anybody, and the other, the private part remaining with the individual; the biometric data with the government or others

will be incomplete and useless, until and unless the private part is supplied by the individual.

**Conclusion**

To conclude, let me reiterate that scientific study is for enhancing the knowledge base for its own sake, while application thereof in real life situation has to take several realities into account, not least the legal requirements. The eminently adorable solutions of the day can be breached or compromised by developments in the scientific study, and hence the applied research needs to constantly revisit the continued relevance of yesterday's best solutions. I am sure this Conference will reflect on the concepts of Identity, Security and Behavioural Analysis from these perspectives. I wish all success for this Conference and great and enriching discussions and debates in this Conference.

Thank you everyone for your patient attention.