Identity and Access Management for the Internet of Things

P. Renee Carnley and Houssain Kettani

***Abstract*—Organizations today gather unprecedented quantities of data from their operations. This data is coming from transactions made by a person or from a connected gadget. From personal devices to industry including government, the internet has become the primary means of modern communication, further increasing the need for a method to track and secure these devices. Protecting the integrity of connected devices collecting data is critical to ensure the trustworthiness of the system. An organization must not only know the identity of the users on their networks and have the capability of tracing the actions performed by a user but they must trust the system providing them with this knowledge. To manage the vast number of devices and feel confident that a machine's identity is verifiable, companies need to deploy digital credentialing systems with a strong root of trust. Traditionally, this has been done with Public Key Infrastructure (PKI) through the use of a smart card. Blockchain technologies combined with PKI can be utilized in such a way as to provide an identity and access management solution for the internet of things (IoT). Improvements to the security of Radio Frequency Identification (RFID) technology and various implementations of blockchain make viable options for managing the identity and access of IoT devices.**

***Index Terms*—Blockchain technology, cloud computing, Identity and Access Management (IAM), Internet of Things (IoT), Public Key Infrastructure (PKI), Radio Frequency Identification (RFID), smart card.**

I. Introduction

Recently, the number of internet connected devices has grown by a third each year, increasing from five billion in 2015 to over twenty billion by 2020 [1]. This stimulates the interest of hackers for competing to enslave an increasing amount of Internet of Things (IoT) devices. Therefore, one of the chief worries is the IoT botnets involved in Distributed Denial of Service (DDoS) attacks. The Mirai IoT botnet that made headlines in 2016 is responsible for the largest DDoS attacks in terms of bandwidth (over 1 Tbps). This instigated the start for investigating solutions for improved security of IoT devices [2]. There are many dangers in regards to an improperly secured IoT device. Given the increase of IoT devices in addition to cloud services that securing the perimeter will remain one of the challenges of cyber-security professionals [2]. This should come as no surprise considering that web-based attacks rated number two in the top threats of 2017 while web application attacks were slightly behind at number three [2].

Internet of Things (IoT) solutions tend to rely heavily on cloud computing. This reliance on cloud computing further increases the need to implement security beyond the normal authentication, access control, and secure channels currently in use. The industry standards requirement to deploy stronger identification, authentication, and authorization is driving demand for trusted digital identities [3].

A chain of trust requires every portion of firmware to be digitally signed before it connects to a network. Once a single item of code has been validated, it can then validate the next portion and so on until every item in the chain has validation. The chain of trust requires a robust foundation at the lowest level that makes it impossible for a malicious user to compromise. This anchor is known as the root of trust. In the most ideal situations, the root of trust is founded on a hardware-validated system such as a Trusted Platform Module (TPM) [4].

Organizations must extend the employment of machine credentialing and methods to practically everything to securely manage their networks. Public Key Infrastructure (PKI) has been around for decades to identify and authenticate individuals and machines. The PKI enables a wide-scale security regime that allows things to have private keys and public key certificates. The PKI holds potential in providing a framework as its security mechanisms that can be used or adapted to support IoT [3]. The IoT is the fastest growing trend motivating the deployment of applications using PKIs. This trend was discovered by the Ponemon Institute's PKI Global Trends Study. The PKI offers a groundwork for developing and handling digital identities at the scale IoT requires [5]. The PKI will soon run on blockchain technology which will make PKI a more robust and trustworthy security method [6].

This paper explores the use of Radio Frequency Identification (RFID) and blockchain technology combined with PKI as an Identity and Access Management (IAM) framework for the IoT. The paper begins with an overview of identity and access management's principles of authentication, authorization, and access control followed by an explanation of the Public Key Infrastructure (PKI). Usage of cloud computing and the types available are described to provide a background for how many organizations are currently utilizing the internet to store, manage, and process data. The paper concludes with an examination of symmetric and asymmetric cryptography near field communication and blockchain technology that may provide a roadmap for how industry can provide a more secure identity and management framework for collecting and exchanging data among IoTs.

II. Identity and Access Management (IAM)

Identity and Access Management (IAM) is generally defined as the framework of policies and technologies that ensure authorized people within an organization have the

Manuscript received April 11, 2019; revised October 30, 2019.

The authors are with the Beacom College of Computer & Cyber Sciences, Dakota State University, Madison, South Dakota 57042 USA (e-mail: houssain.kettani@dsu.edu).

doi: 10.18178/ijfcc.2019.8.4.554

appropriate access to network resources. Identity management systems provide access control to an organization's resources and monitor user activity while active within those resources [7]. The IAM provides a means to manage user authorizations based upon their role within the organization. This is done by delivering a means of protecting organization resources and data through rules and policies requiring login passwords, defining user privileges, and governing user accounts [8].

A. Authentication

Authentication contributes information as to the identity of a user. An authentication system will verify a user's credentials to allow access to protected resources. These credentials require strong authentication such as two or more factors like fingerprint, one-time password, and the use of a token. This is usually referred to as multi factor authentication [8].

B. Authorization

Authorization ensures that the user only has access to the services and resources to which they are entitled. These privileges are based on roles granted by an organization. Roles should be assigned per company policies that enforce guidelines for the approval or disapproval of access [8].

C. Identity Management

The system that manages the establishment of a digital identification or account which an employee is assigned upon hire is identity management [8]. This system manages the digital identity of a user as well as their passwords, tokens, or other methods of identification [7]. It is critical that access be revoked upon a user terminating employment [7], [8].

D. Federated Identity Management

Authentication and authorization requires strong trust in a system to accurately identify and allow access to resources. The trust established between multiple applications or organizations is called Federated Identity Management (FIM). The FIMs are usually third-party providers that store user information and credentials which allow single sign on (SSO) without passwords. Industry standards that provide FIM include but are not limited to Security Assertion Markup Language (SAML), Open Authorization (OAuth), and OpenID [8].

III. Public Key Infrastructure (PKI)

The authentication and authorization validation process of an IAM requires strong trust that must have meaning and be quantifiable [9]. Since trust is more of a social construct, giving it meaning and finding measurements within an electronic system proves challenging [10]. Public Key Infrastructure (PKI) has sustained itself since last century as the de facto standard for providing electronic trust within a centralized management system. The PKI's reliability on the correct usage of a public/private key pairs depends upon there being a chain of trust among Certificate Authorities (CA). A public key certificate is issued as the public component of these key pairs and are often associated with a smart card. These CAs are the third-party servers providing the certification path to authentication. Path validation and path construction are essential to the proper management of trust within PKI [10].

A. Path Validation

Prior to allowing a user access to a system or network, the authenticity of the public key presented must be assured. A Validation Authority (VA) is a trusted server providing means of verifying the validity of a digital certificate. The trusting entity sends a certificate to the VA server that validates the Public Key Certificate (PKC). This process typically occurs on the client side and requires the use of software that can support the protocols and algorithms. An organization's use of a VA in addition to establishing policies provide confidence in who is and who is not allowed on their systems [11].

B. Path Construction

Path construction is the process of building a CA certification path. Constructing this path is generally more difficult than path validation [10]. These paths are defined and based upon the X.509 PKI standard [12]; further details can be gleamed from examination of that standard. Path construction typically begins with a root CA that generates its own self-signed certificate. Once the root CA is established it binds the identity and public key of an intermediate CA. The intermediate CA launches the next CA in the path and so on and so on until the path reaches the end-user who seeks a certificate [10].

IV. Cloud Computing

Cloud computing is becoming more and more popular as a business model where users pay solely for the resources they use. This allows for a more flexible and cost-effective computing environment. Most business' including the government have moved to the cloud. Governments and organizations that use to house expensive onsite data centers are relying on cloud solutions. The cloud offers lower cost and better services through virtual machines running within hypervisors. The National Institute of Standards and Technology (NIST) outlines four primary cloud computing models; private cloud, community cloud, public cloud, and hybrid cloud [13].

A. Private Cloud

A private cloud provides Information Technology (IT) solutions to a single individual or business that have unique or unpredictable computing needs [13]. These cloud servers are typically run within the owner's data center utilizing proprietary architecture but may use a third party's cloud infrastructure. It may be on or off the premises, managed and operated by the organization, and the organization maintains control of the cloud [13].

B. Community Cloud

A community cloud comprises a cloud infrastructure set up for the use by a group of organizations that have common interests. The US DoD provides a good example of a community cloud as they share joint mission, security requirements, policies, and compliance considerations. The

cost of a community cloud can be split among all users and managed by one member of the community while allowing access to all authorized members [13].

C. Public Cloud

A public cloud is a third party that provides computing services for the general public. This cloud is available to anyone with cloud computing needs and resides on the premises of the cloud provider. This cloud is typically owned and managed by a third party, multi-tenanted, and is a pay per usage by the user [13].

D. Hybrid Cloud

A hybrid cloud is a mix of two or more of the other cloud computing types. The hybrid gives greater flexibility and better cost effectiveness than the other cloud modeling types. It can take the best benefits from each reducing the overall weaknesses that may be found in the others [13].

V. Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) technology is a low powered system that transmits wirelessly. The tags are generally passive devices meaning they have no power source while the readers are a more complicated computing device with sufficient power, memory, communication interfaces, and its own clock. Beginning as a mechanism to replace barcodes, RFID blossomed to include a wide variety of applications such as toll transponders, passports, credit cards, access badges, pet tracking devices, pharmaceuticals, clothes, library books, and much more [14]. This has led to RFID becoming the preferred method of providing wireless communication between IoT devices. This has increased the need to commission a secure method of authentication and IAM. Electronic Product Code Class 1 Generation 2 (EPC C1 G2) standard is the most widespread RFID standard projected to provide secure authentication for RFID users [15].

Lightweight authentication protocols incorporating simple cryptographic functions have been developed to provide an authentication method. The RFID systems incorporate RFID tags and RFID readers. To utilize a PKI IAM, each tag needs its own public/private key pair with a public key certificate. The primary purpose of RFID tags is to allow identification by readers. A reader that has become the possession of a malicious user (i.e. stolen, lost, compromised) can be used to identify and track tags. Therefore, it is more critical to have trust in the reader than the tag. One possible way of providing trust despite the risks associated with the reader is via near field communication [14].

A. Symmetric Cryptography

Near Field Communication (NFC) is a more simplistic implementation of the RFID technology. The NFC involves two wireless devices operating via short range frequencies within 5-10 cm. There are two modes: active and passive. An active mode device starts the communication. These devices are referred to as the initiator. The initiator generates its own power and sends information by amplitude shift keying. Within passive mode the device is referred to as the target and uses the Radio Frequency (RF) field from the initiator as power for its communication [16]. Within NFC, the lines between reader and tag are blurred eliminating the primary issues of RFID PKI usage. For example, NFC-enabled smartphones can switch between being a reader and being a tag. While sending the smartphone acts as the tag and while receiving it acts as the reader. A cryptographic challenge response protocol based on PKC and PKI has been developed for protecting NFC tags from attacks. This proposed framework consists of using symmetric cryptography [17].

To enhance security, a secure protocol is presented with the NFC chip [16]. The intent is to add an extra layer of security within NFC-enabled systems by incorporating a data/information processing unit. The security protocol includes a processing stack. This stack consists of handshaking, scheme, certificate verification, signature verification, and an alert mechanism [17]. The process begins by the handshaking scheme asking for a certificate. If the certificate and the signature match, data is stored for further processing [17]. If at any time there is an error i.e. the certificate and the signature cannot be verified, the data is discarded from the system and alert messages are transmitted [16]. The proposed NFC system was tested and found to adequately protect against tag manipulation and data insertion. There are minor increases to the processing time the larger the signature size used. Thus, to save processing time use a smaller signature [17].

B. Asymmetric Cryptography

Robust authentication is a requirement for IAM. Most leading services provide strong authentication through symmetric cryptography such as Advanced Encryption Standard (AES) or asymmetric cryptography such as Elliptic Curve Cryptography (ECC) [18]. Asymmetric solutions such as ECC are complex to implement and often inefficient. Researchers have discovered a secure NFC with a flexible architecture call Cryptographic Protected Tags (CRYPTA). The latter works passively using a low-area design that utilizes as few resources as possible. This passive implementation provides a secure NFC/RFID that may be used in IoT devices such as NFC-enabled smart phones [18].

Authenticity and confidentiality are used to provide end-to-end communication between a client and a server, therefore a server is required to authenticate its identity to a client and vice-versa [9]. The CRYPTA tag provides strength in authentication through an analog antenna that demodulates and modulates the data, extracts the power supply, and provides a stable clock and reset signal [18]. The framing logic is the portion that handles the time critical low-level commands. The cryptographic operations are processed within the crypto unit and is accessed by the microcontroller via micro-code patterns. The tag's power is supplied from the RF field and provides the interface for the data, clock, and reset. Smart cards often use 32-b controllers that have high area and power consumption, CRYPTA uses an 8-b microcontroller with a low chip area and low power consumption making CRYPTA more efficient than anything currently in use [18]. The only downside to CRYPTA is that it is a proposed real-world RFID system that includes all hardware components needed for a practical chip fabrication.

While the scientists who designed the system invented a prototype that tested well in the lab [18], more testing will be needed to prove the viability of it as an IoT solution.

VI. Blockchain Technology

A blockchain is a data structure that utilizes public-key cryptography in the development of tamper-proof digital signatures that may be shared among parties. Basically, they are online ledgers that provide decentralized and transparent data sharing [19]. Blockchains are the technology behind bitcoins that have been successfully used in E-commerce. Blockchains rely on cryptographic proof instead of trust negating the use of a trusted third-party and allowing anonymity in online transactions [6]. In order to affectively implement blockchain within IAM, establishing trust would be necessary to instantiate security measures against interference, breach, and eavesdropping [20]. A considerable vulnerability to IoT applications and platforms is their dependence on a centralized cloud. The PKI in its current form is centralized relying on trusted third-parties. Decentralizing and incorporating blockchains provides the means of overcoming several of the problems linked with the centralized cloud approach. Provenance and other startups are using blockchain to promote trust in product transactions from source to the customer [19].

Filament is a blockchain IoT solutions provider that has introduced wireless sensors, called Taps, that allow communication with computers, phones, or tablets within ten miles. Taps are connected in a decentralized system using autonomous smart contracts that are blockchain based allowing IoT devices to communicate securely and exchange data safely [19]. A smart contract is a digital contract written by source code and executed within the tamper-proof construction of blockchains [21]. Blockchains can cryptographically sign transactions and verify the originator's cryptographic signature to guarantee a message's origin [19]. Blockchains also provide secure traceability of certifications and other relevant data in supply chains. Blockchain's public availability ensures transactions can be linked to identify vulnerable IoT devices [20]. Suitable for registering time, location, price, parties, and data as they move through the supply chain, blockchain based IAM systems will help strengthen IoT security [19].

A. Ethereum

Ethereum is an open-source blockchain platform providing an infrastructure that developers can use to produce applications in an open and decentralized platform. Ethereum is considered incorruptible since third-parties cannot modify data and secure with error avoidance due to the decentralized applications being preserved by entities rather than individuals. This system would be permanent because blockchain continues to operate even if a computer or server crashes [21].

B. Blockchain-Based PKI

A PKI framework as it currently exists has vulnerabilities. Reporting unauthorized certificates is time consuming and labor intensive leaving a CA open to a man-in-the-middle (MITM) attack. If the CA's are not operating correctly, the introduction of encryption has no value. Blockchain-based PKI techniques such as Instant Karma PKI (IKP) as well as others provide a method to correct the CA vulnerabilities immediately in real time [22]. Transport Layer Security (TLS) currently safeguards much of the encrypted client-server communication traveling over the internet. The IKP would be implemented as an extension of TLS with detectors and IKP authority [22]. The IKP authority consists of the core functions of IKP such as the CA identifiers and the public keys used for authentication. Domain certificate policies (DCPs) that compute the authorization of a certificate and the reaction policies (RPs) that automate responses to unauthorized certificates are stored within the IKP authority [18].

The IKP model provides incentives for DCP compliance and misbehavior reporting as certificates are issued that comply with a domains DCP or a certificate is reported if it violates a domain's DCP. The IKP authority is instantiated as a smart contract called the IK contract within Ethereum that does not need to be trusted. Ethereum provides a natural computation platform that allows checker and reaction algorithms within IKP [18]. Blockchain-based PKI supports the revocation of the certificate that is an issue in the traditional PKI systems. Within blockchain-based PKI the validation of a certificate is simple and fast. PKI based on Ethereum's smart contracts make MITM attacks virtually impossible because when a CA is published or revoked, the information is distributed across thousands of nodes. A blockchain-based PKI framework mitigates the problems of the traditional PKI and reduces maintenance costs [6]. The ability to report and respond to CA misbehavior automatically improves security [18].

VII. Concluding Remarks

The IoT will remain unmanageable and insecure without a system of trust. Industry wants to know who is connecting to their networks and what they are doing while on their networks [17]. If industry is to protect themselves from the biggest threats they face today, an effective IAM for IoT must be established. This paper presents solutions that promise an answer to providing an IAM for IoT. A clear path to follow in establishing a blockchain-based PKI IAM for IoT can be realized with just a little more test and analysis of the proposed systems. Instead of a CA server that requires backups, maintenance, and updates, the CA will be built on a blockchain running on thousands of computers simultaneously. Ethereum provides a decentralized and infrangible global computing system that doesn't rely on third-parties which provides the means to incorporate a chain of trust within a blockchain-based PKI framework utilizing RFID. Any future work should include an integration with cloud computing as more and more of industry moves to the cloud [17]. The future of IoT IAM is addressed in the blending of existing technologies.

References

[1] S. Ganguli and T. Friedman. (2017). *IoT Technology Disruptions: A Gartner Trend Insight Report (Report ID G00331334).* [Online].

Available: https://www.gartner.com/en/doc/3738060-iot-technology-disruptions
[2] European Union Agency for Network and Information Security (ENISA). (2018). *ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends*. [Online]. Available: https://doi.org/10.2824/967192
[3] F. J. M. Thomas, J. S. Pasquier, and J. Bacon, "Clouds of things need information flow control with hardware roots of trust," in *Proc. IEEE 7th International Conference on Cloud Computing Technology and Science*, Vancouver, BC, Canada, 2015, pp. 468-470.
[4] V. Zimmer and M. Krau, (2016). *Establishing the Root of Trust*. [Online]. Available: http://www.uefi.org/sites/default/files/resources/UEFI%20RoT%20white%20paper_Final%208%208%2016%20%28003%29.pdf
[5] J. C. Asenjo, *Three Reasons why You Need a Root of Trust when Orchestrating Machine Identities*, San Jose, CA: Thales eSecurity, 2017.
[6] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983-994, 2017.
[7] M. A. Thakur and R. Gaikwad, "User identity and access management trends in IT infrastruture–An overview," in *Proc. International Conference on Pervasive Computing (ICPC)*, Pune, India, 2015, pp.1-4.
[8] A. Sharma, S. Sharma, and M. Dave, "Dentity and access management –A comprehensive study," in *Proc. International Conference on Green Computing and Internet of Things (CGCIoT)*, Noida, India, 2015, pp. 1481-1485.
[9] S. Matsumoto, R. M. Reischuk, P. Szalachowski, T. H. Kim, and A. Perrig, "Authentication challenges in a global environment," *ACM Transactions on Privacy and Security*, vol. 20, no. 1, pp. 1-38, 2017.
[10] P. P. Rahoof, L. R. Nair, and T. Ijyas, "Trust structure in public key infrastructures," in *Proc. 2nd International Conference on Anti-Cyber Crimes (ICACC)*, 2017.
[11] Y. Ma, "Research on the solution of PKI interoperability based on validation authority," in *Proc. International Conference on Computer Science and Service Ssytem (CSSS*), Nanjing, China, 2011, pp. 697-700.
[12] Telecommunication Standardization Sector of ITU. (2016). Recommendation ITU-T X.509. *Series X: Data Networks, Open System Communications and Security*. [Online]. Available: https://www.itu.int/rec/T-REC-X.509/
[13] M. Denis, J. C. Leon, E. Ormancey, and P. Tedesco, "Identity federation in openstack – an introduction to hybrid clouds," *Journal of Physics: Conference Series*, vol. 664, no. 2, 2015.
[14] D. Gritzalis, R. Nithyanand, G. Tsudik, and E. Uzun, "User-aided reader revocation in PKI-based RFID systems," *Journal of Computer Security*, vol. 19, no. 6, pp. 1147-1172, 2011.
[15] B. Abdolmaleki, K. Baghery, B. Akhbari, and M. R. Aref, "Cryptanalysis of two EPC-based RFID security schemes," in *Proc. 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, Rasht, Iran, 2015, pp. 116-121.
[16] A. Asaduzzaman, S. Masumder, and S. Salinas, "An auspicious secure processing technique for near field communication systems," in *Proc. IEEE 7th Annual Ubiquitous Computing, Electronics, & Mobile Communication Conference (UEMCON*), New York, 2016, pp. 1-6.
[17] A. Asaduzzaman, S. Mazumder, S. Salinas, and M. F. Mridha, "A security-aware near field communication architecture," in *Proc. International Conference on Networking, Systems and Security (NSysS)*, Dhaka, Bangladesh, 2017, pp. 33-38.
[18] T. Plos, M. Hutter, M. Feldhofer, M. Stiglic, and F. Cavaliere, "Security-enabled near-field communication tag with flexible architecture supporting asymmetric cyptography," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 11, pp. 1965-1974, 2013.
[19] N. Kshetri, "Can blockchain stregthen the internet of things," *IT Professional*, vol. 19, no. 4, pp. 68-72, 2017.
[20] C. Robey, "Whom do you trust? Part 2 blockchain technology & smart contracting," *Contract Management*, McLean, VA: National Contract Management Association, 2017.
[21] J. Cheng, L. Narn, C. Chien, and C. Yi-Hua, "Blockchain and smart contract for digital certificate," in *Proc. IEEE International Conference on Applied System Innovation*, Chiba, Japam, 2018, pp. 1046-1051.
[22] S. Matsumoto and R. Reischuk, "IKP: Turning PKI around with decentralized automated incentives," in *Proc. IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2017, pp. 410-426.

P. Renee Carnley was born in Pensacola, Florida, USA. She received the B.S. degree in Computer Engineering from the University of Florida, Gainesville, Florida, USA, M.S. degree in Computer Science from the University of West Florida, Pensacola, Florida, USA, and is currently pursuing her Ph.D. in Cyber Security from Dakota State University. Ms. Carnley works full time for the Air Force Special Operations Command (AFSOC) located at Hurlburt Field, Florida, USA as their Senior Software Engineer. She is the Project Manager for a software team that develops software for Command and Control (C2) Systems, the AFSOC Cloud, and other diverse projects for command staff and the warfighter. Her team's software provides situational awareness, secure & effective mission communications, and productive tasking of resources. She holds certifications in AWS Cloud Services, CompTIA Security+ and the International Information System Security Certification Consortium (ISC^2) Certified Information Systems Security Professional. She is a member of the Society of Women Engineers (SWE), Institute of Electrical and Electronics Engineers (IEEE), and the National Center for Women & Information Technology (NCWIT).

Houssain Kettani was born in Khobar, Saudi Arabia, in 1978. He received the B.S. degree in Electrical and Electronic Engineering from Eastern Mediterranean University, Cyprus in 1998, and M.S. and Ph.D. degrees both in Electrical Engineering from the University of Wisconsin at Madison in 2000 and 2002, respectively. Dr. Kettani served as faculty member at the University of South Alabama (2002-2003), Jackson State University (2003-2007), Polytechnic University of Puerto Rico (2007-2012), Fort Hays State University (2012-2016), Florida Polytechnic University (2016-2018) and Dakota State University since 2018. Dr. Kettani has served as Staff Research Assistant at Los Alamos National Laboratory in summer of 2000, Visiting Research Professor at Oak Ridge National Laboratory in summers of 2005 to 2011, Visiting Research Professor at the Arctic Region Supercomputing Center at the University of Alaska in summer of 2008 and Visiting Professor at the Joint Institute for Computational Sciences at the University of Tennessee at Knoxville in summer of 2010. Dr. Kettani's research interests include computational science and engineering, high performance computing algorithms, information retrieval, network traffic characterization, number theory, robust control and optimization, and Muslim population studies. He presented his research in over seventy refereed conference and journal publications and his work received over five hundred citations by researchers all over the world. He chaired over hundred international conferences throughout the world and successfully secured external funding in millions of dollars for research and education from US federal agencies such as NSF, DOE, DOD, and NRC.