Systematic Review of Identity Access Management in Information Security

Mumina Uddin and David Preston

Abstract—**This report is a systematic review on Identity Access Management (IAM) in information security. Objective of this report is to identify the intensity of the research on IAM solution, which particular Taxonomy of security has been researched upon most and the area under-researched . Data source were original articles written in English found in IEEE explore, Science Direct, ACM Digital Library, Google Scholars. Study selections were articles related to Identity access management / Access Control within the information security, information management area. Article excluded that were industry specific and role engineering. Data extracted by search engine using predefined search string which contain 127 articles, it was reviewed manually using the title and the abstract initially using the predefined eligibility criteria. A total of 40 articles were selected for the purpose of this study, after screening through detailed reading of the articles a total of 18 articles selected for the review. It revealed IAM solution has not been adopted efficiently it is an emerging technology and have received interests from wider organization. Data security, Compliance has been researched most due to the security breach, data loss incidences. Bring it your own (BOYD) security within personal mobile technology have posed threats and vulnerabilities, security awareness, policy and best practices have thought to be the factors contributing to the failure in information security. It is the technology, people and process needs to work coherently to have secure information system.**

Index Terms—**Information security, identity access management, articles.**

I. Introduction

ICT environment has created mixed approach to access management across sectors. Web based, remote access coupled with applications access distributed on various networks and hosted on cloud. Enterprises are faced with various challenges with the administrative issues, data privacy, increase operation burden, monitoring issues and the regulatory compliance. In order for the organization to sustain competitive edge, it requires firm internal controls. This is only possible where the organization have streamlined internal processes.

Identity management is widely herald as an opportunity for enhancing the operational process in information security, reducing cost, enhanced reporting capability and regulatory compliance. However in recent year this has proven to be the concept misunderstood, complex and costly.

A. Identity Access Management (IAM)

"Identity is the new perimeter in the organization," says Colin Bannister, VP and CTO, CA Technologies UKI [1]. Identity has become the key in a de-parameterized world. Effective identity and access management (IAM) enables open interaction between a business and employees, consumers or customer and partner organizations. Identity access management concept is evolving; it has been implemented unsuccessfully up until now. According to Quocirca, 65% of UK businesses surveyed have opened up applications to users from customer organizations, consumers or both 7% above the European average [1]. Many organizations are still reliant of manual provisioning of information access, user access addition, removal and update. This leave user under-privilege or over privilege access, high risk of human error and this could open up the organization fraud risk.

B. Traditional Identity Access Management (IAM)

IAM access were initial thought of a departmental issue such as information security issue, in the second wave of IAM it is now understood that the IAM is the business as a whole issue. In order for IAM to work effectively, business units will need to work together. Various vendors past have tried in the past to sell off the shelf products, which were unsuccessfully implemented [2], [3]. This has led to plastering the broken system as opposed to fixing the issue itself. Due to business expansion and application open access needing to provide to internal and external client, it has become apparent that an identity solution is vital to survive the competitive market and have strong security solution.

Auto-provisioning tool (IAM) had been implemented unsuccessfully. Only process automated was the creation/deletion of the new user accounts in Active Directory. Users were provisioned manually into other banking applications. This tool not only added extra steps into the administration workloads also left administrators to fix incomplete account creation. Once the automated tool was executed administrators were left to wait considerable amount of time for the account creation process to complete. This was very difficult when an urgent account access needed to be setup.

C. Cloud Based Identity Access Management (IAM)

Second wave of Identity access management is the cloud based Identity Access management, Opening of increase level application to external user, use of cloud based services and rising use of social media requiring access to application. Increased number of IT infrastructure is either SAAS or Cloud based. The perimeter is now shrinking; IAM solution need embrace social, mobile and the cloud. IAM solution is not just about networking, it about identity-based control of data. It needs to secure whether it is sent to cloud or mobile. Identity and entitlement are keys to the encryption of data; they will ensure that only people with the entitlements can only access the data.

Manuscript received August 10, 2014; revised March 13, 2015.

Mumina Uddin and David Preston are with the University of East London, Chingford, UK (e-mail: u1146764@uel.ac.uk, d.preston@uel.ac.uk).

DOI: 10.7763/JACN.2015.V3.158

Disadvantage with SaaS and the cloud, often organizations are being downgraded to 'one size fits all' security [4]. This lack of granular control and auditing is currently preventing CIOs in regulated industries from benefiting from the productivity and scalability of SaaS, according to Richard Walters, CTO of SaaS ID, who believes that, "At the moment, the cloud represents a blind spot for CIOs. They can see when employees have logged in and logged off, but they cannot see what was done in between. In addition, they have no way of auditing interactions with web applications". Information security management department is responsible for administering, monitoring and assurance of access to information within the Bank, both internal premises and application hosted on cloud. It is vital that the information is available when required providing both integrity and confidentiality. Failure to deliver information on time, lacking in integrity could results in compensation, loss of business, disclosure of company secrets and compliance issues. In order to have a better security system there needed to be control and enforcement [5]. Both people and technology needed to work coherently to have a secure system. Change control needed in a controlled manner with all the stakeholders working as a whole [6].

Sarbanes Oxley act (SOX) compliance certification requires accuracy of financial statement and firm internal controls. Section IV states that an annual assessment of internal controls over financial reporting obtaining attestation from external auditors. Section III requires CEO/CFO accuracy of their financial statements. Enterprise wide auto provisioning is the key component for companies to meet the requirement of Section III and Section IV SOX act for the CEO and CFO to demonstrate that their business processes are under control.

II. Objectives

1) The objective of this report is to perform a systematic literature review on Identity access management in information security. In order to answer the following research question;
2) What is the intensity of research activity on framework/model/best practices for IAM Solution in information security?
3) What IAM security functional taxonomy is being addressed in IAM development?

Which IAM security Taxonomy has been under-researched?

This report looks at the IAM information security related published literature, it may have predefined functional security requirement provided by the vendors which may not reflect the real identity access management solution that are not meeting the enterprises security requirements.

This review would provide useful contribution for the stakeholders as well as the vendors, third party services, auditors, consultants. This review aiming at the financial sectors, it could be beneficial for government, defense, healthcare, education systems.

III. Methods

This review used systematic review to ensure that the search and the retrieval process have been accurate and impartial. This systematic review has followed the quality reporting guidelines set by the preferred reporting items for Systematic reviews and Meta-Analysis (PRISMA) group [7].

A. Eligibility Criteria

The following inclusion criteria were used: articles that are written in English, articles related to the research questions: Identity access management, Identity access control within the information security and security management field.

B. Information Sources

The research was applied to GOOGLE Scholars, IEEE explore, Science Direct, ACM Digital Library, Date between 2010-2013 and the references. Included in the articles have also been scanned to obtain to ensure review is fully comprehensive.

C. Study Selection

The study selections were organized using the four phase:

1) Research publication related to Identity access management and Access control. This phase was searched using the string ("Identity access management") AND ("Access Control "OR solution"), which was adapted to the search engine.
2) Exploration of Title, abstract, identified key words and selection based on the eligibility criteria
3) Complete and partial articles that had not been eliminated were read to identify whether it is related to the eligibility criteria.
4) Scanning the reference list to identify whether there were new studies provided it meets the eligibility criteria. Excluded publications that were Role engineering models, architectural details of IAM solutions.

D. Data Collection Process

An evaluation revealed search engine Science Direct and IEEE Explore are best source for the purpose of the topic in this report; after initial search it followed 4 steps:

1) Query selection and search engine, initial search on identity access management revealed 20,962 articles in various sectors from the date ranging from 2010-2013.
2) Manual refinement revealed that not all articles related to the objectives of this report they were identity related to social sciences, medicine, tourism and computers in human behaviour, IDM software development and various role based models of the information security.
3) Extension and verification, each article was then checked for the title, abstract and the content to include and exclude based on the eligibility criteria.
4) Classification of relevant publication, classification of the publication was based functional areas of security, data security, auditing, assurance, provisioning, compliance, policy and governance

IV. Results

A search on the identity access control topic revealed 21332, which entails various field of social sciences, medicine, human behaviors, women health organization, tourisms and teaching. This search has searched for all

articles in "identity" and "control". After filtering the research limited to "information security" and Information management and access control revealed total of 172 articles (Table I). It was then filtered further by the topic "information security". After the screening of the title, abstract, and the publisher 40 articles were thought to be appropriate for the systematic review. Those that were thought to be relevant for the research questions set in this article and meet the eligibility criteria were manually read through and classified based on security domain (Table III). 10 records were excluded based on either the article specific to security for certain organization, specific to security threat incidence analysis and cloud services security related. Remaining 30 articles were then read thoroughly taken out ones emphasizing more on software vulnerabilities, cybercrime, stock market threat report, individual vendor security report and that has remain 18 articles. Those articles then subdivided into what is qualitative and quantitative, 14 reports were qualitative ad 4 were quantitative. Qualitative are the one process related and more theory based, quantitative are the one that collated market data, comparisons and provided figures and facts. Fig. 1 below shows how articles were identified screened, to obtain articles relevant to this systematic review objective.

TABLE I: THE SUMMARIZING THE ARTICLE RETRIEVED USING KEYWORDS

Search Engine	String	No of articles	Publication date
Science Direct	ALL(identity access management) AND LIMIT-TO(topics, "access control, information security") AND LIMIT-TO(topics, "access control, information security") AND LIMIT-TO (pubyr, "2013")	**44**	**2013**
Science Direct	ALL(identity access management) AND LIMIT-TO(topics, "access control, information security") AND LIMIT-TO(topics, "access control, information security") AND LIMIT-TO (pubyr, "2013,2012,2011")	**114**	**2011-2013**
Science Direct	ALL(identity access management) AND LIMIT-TO(topics, "access control, information security") AND LIMIT-TO(topics, "access control, information security, security management")	**380**	**1994-2014**
Science Direct	ALL(identity access management) AND LIMIT-TO (contenttype, "1,2","Journal") AND LIMIT-TO(topics, "access control, information security") AND LIMIT-TO (contenttype, "1,2","Journal") AND LIMIT-TO(topics, "information security") AND LIMIT-TO (pubyr, "2013,2012")	**14**	**2012-2013**
Science Direct	ALL(identity access management) AND LIMIT-TO(topics, "access control, information security") AND LIMIT-TO(topics, "access control, information security, security management") AND LIMIT-TO(pubyr, "2013,2012,2011") AND LIMIT-TO (contenttype, "1,2","Journal")	**65**	**2011-2013**
IEEE Explore	ALL(identity access management)AND LIMIT-TO (pubyr, "2010,2011,2013")	**8**	**2010-2013**

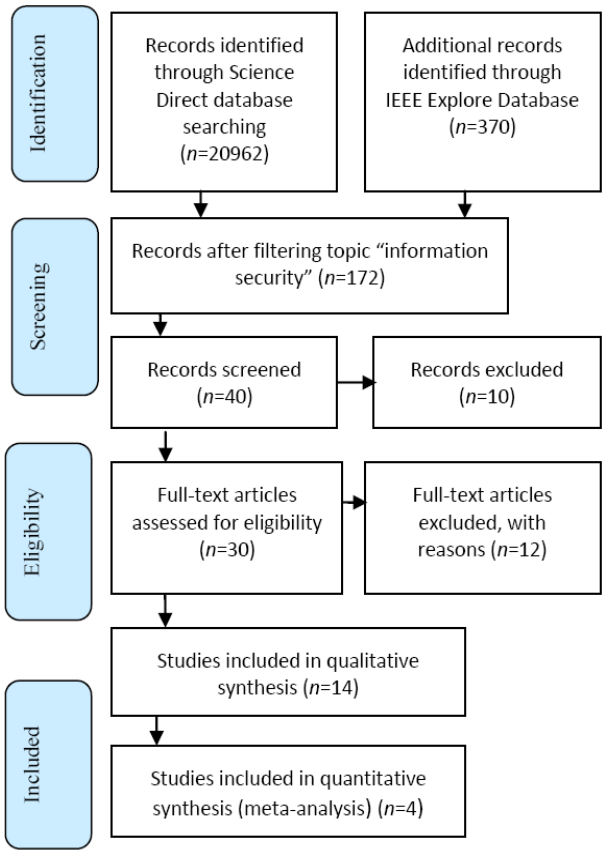

Fig. 1. Eligibility screening of articles.

TABLE II: TAXONOMY OF IAM

	Security Domain	Subgroup
	Data Security:	Data Storage: transit or still
		Privileged Account Management
		Mobile data
		Data Model
IAM	**Provisioning**	IAM frameworks
		Cloud based IAM framework
		IAM Standard
	Compliance/Policy	Data workflow
		Security Awareness
		Audit

V. ANALYSIS OF RESULTS

As shown in the (Table VI) research emphasis were on data security, policy and security awareness. During 2011, compliance, cloud security and IAM software research has been focused on top of data security. In the year 2013, security assurance, IAM standard, Security workflow has been focused on more. Data security has been the main focused of information security throughout the years, as organization critical assets it is its data.

It is also noticed that main publishers were computer security & fraud and the network security. Between 2010-2013 computer fraud & security have published 7 articles (Table IV) related to this systematic review covered in various security sub groups, including a systematic review on role modeling, information life cycle framework [4], unrealistic optimism of the management of information security [8], IAM solution review and mistakes were highlighted [9], Bring it your own mobile device (BOYD)

possessing threats and security awareness [10], [11]. SCIM work in progress for API standards for cloud based IAM system and finally a security review of threats and future [12]. Computer fraud & security looked at the security domains in various angels and highlighted issues in various areas of security domains which make up the IAM.

Second dominant publisher was network security, there was 6 articles published between 2010-2013 (Table IV), articles main focused were on encryption of data [13], privileged accounts, roots accounts, segregation of duties, highlight on why the traditional approach to security is not working, information security without boundaries [14], black hole business security emphasis on managing data loss policy, hybrid cloud security on public and private, brief on types of cyber threat aiming at the data [15].

TABLE III: PUBLICATION BY MAJOR PUBLISHER COMPUTER FRAUD AND SECURITY

Author	Year	Publisher	Title	Weakness	Strength	Security Domain
Vrhovec, Grega,	2011	Computer Fraud & security	Beating the privacy challenge	Very brief overview and not specific to any regulatory body.	Emphasis on the legislation, data privacy and compliance.	Compliance
Lewis, Nick	2012	Computer Fraud & security	Access rights – protect access to your data or lose it: serious misconceptions about information security,	Issues has been identified no resolution provided or available.	Using the expert knowledge author was able to identify a critical issue within data security	Compliance, Data Security, Auditing
Mansfield-Devine, Steve,	2013	Computer Fraud & security	Security review: The past year	Review on mobile devices not proposed solution	Emphasis on BYOD devices, mobile devices posses threat, data security	Data security, security Awareness, Cloud Security
L. Fuchs, G. Pernul, *et al*.	2011	Computer Fraud & security	Roles in information security – A survey and classification of the research area	Mostly theoretical concepts	Access control model concept, insight and future	Data Security, policy and Standard
Spencer, Travis,	2012	Computer Fraud & security	Identity in the Cloud	Brief outline of the solution, not has been tested, onion expressed	Standardized framework proposed, (IETF) for further development	IAM Standard, cloud Security
Rhee Hyeun-Suk, U. Ryu Young *et al.*	2012	Computer Fraud & security	Unrealistic optimism on information security management	Optimistic bias and risk management behavior not been s	Critical issue within information security optimistic bias	Security Awareness,
Caldwell, Tracey	2013	Computer Fraud & security	Identity –the new parameter	No solution provided as IAM solution is large	Review on IAM solution been implemented and flaws,	Workflow, Data Security, policy

TABLE IV: PUBLICATION BY MAJOR PUBLICATION NETWORK SECURITY

Author	Year	Publisher	Title	Weakness	Strength	Security Domain
Dinoor, Shlomi,	2010	Network Security	Privileged identity management: securing the enterprise Network	brief outline of issue with privileged account	Privilege centric approach framework	Data Security
Hart, Jason	2013	Network Security	Why the traditional approach to information security is no longer working	Biased, author cloud solution worker safenet, this is theoretical works and not tested	Analyses weakness in security, supported with statistics	Data Security and Policy
Caldwell, Tracey	2013	Network Security	Security at the data level	Lacking detailed description of the methods	Group of experts in their fields, methods of securing data in various environment	Data Security and Security Awareness
Blandford, Richard	2011	Network Security	Information security in the cloud	Theoretical and not very detailed	Another framework for information security on cloud	Data Security, Cloud security
Durbin Steve,	2011	Network Security	Information security without boundaries	Overview of what could be secured, not very specific.	Framework for data security network, application and devices	Data Security, Cloud security
In Brief,	2011	Network Security	In Brief	Not very detailed,	Past threat on data security	Data Security, compliance

TABLE V: LITERATURE PUBLISHED ON SECURITY DOMAIN

Author	Year	Publisher	Security Domain
Vrhovec, Grega ,	2011	Computer Fraud & security	Compliance
Lewis, Nick	2012	Computer Fraud & security	Compliance, Data Security, Auditing
Mansfield-Devine, Steve,	2013	Computer Fraud & security	Data security, security Security Awarenes, Cloud
L. Fuchs, G. Pernul, et al	2011	Computer Fraud & security	Data Security,policy and Standard
Spencer, Travis,	2012	Computer Fraud & security	IAM Standard, cloud Security
Rhee Hyeun-Suk, U. Ryu Young.et al	2012	Computer Fraud & security	Securiy Security Awarenes,
Caldwell, Tracey	2013	Computer Fraud & security	Workflow, Data Security, policy
Courtney, M.,	2011	Engineering & Technology	IAM software, Data Security, compliance, Cloud
Everett, Cath,	2011	IAM Vendor Marketwatch	Data Security, workflow,policy
Bunker, Guy,	2012	Information security Technical report	Assurance
Pritchard, stephen,	2010	Infosecurity	Security Awarenes and policy
Dinoor, Shlomi,	2010	Network Security	Data Security
hart, Jason	2013	Network Security	Data Security and Policy
Caldwell, Tracey	2013	Network Security	Data Security and Security Awarenes
Blandford, Richard	2011	Network Security	Data Security, Cloud security
Durbin,Steve,	2011	Network Security	Data Security, Cloud security
In Brief,	2011	Network Security	Data Security, compliance
Alotaibi, S.J. ; Wald, M.,	2012	World congress on(WorldCIS)	IAM software

TABLE VI: SHOWS THE RESEARCH ACTIVITIES IN VARIOUS SECURITY DOMAINS BETWEEN 2010-2013

Security Domains	Information covered in articles	Percentage %
Assurance	1	3
Compliance	3	8
Data Security	12	33
IAM software	2	6
Security Awareness	4	11
Workflow	2	6
Policy	5	14
Standard	2	6
Cloud Security	5	14
Total	36	100

A. Identity Access Management (IAM)

IAM refers to digital identity in a corporate environment needs to be treated with high priority. Irrespective of different applications/platforms use in organization, resources need to be managed and allotted to the appropriate identity/user (i.e. provisioning management) with proper access rights (access/policy management). This process is called identity management [16]. Identity access management encompasses of three functional areas; data security, provisioning and compliance.

B. Data Security

As shown in (Table II) for the year 2010-2013, data security has been classified based on subgroup of security domain, data in transit or still, data storage , data model and privileged accounts access data. Data in transit or still will needs to be protected to avoid data breach. [5] Security the data and not the organization. As show in (Table VI) 33% of all the articles selected contained research on data security. Cloud security has been sub grouped with data security as this is mobile data storage and it comprises to 14% of all articles researched (Table VI). Combining the data security and the cloud security it is a total of 47% of articles containing research on data security. Although there is a high number of research on data security, it is remained the research area under-researched as the technology evolving and new research areas emerging such as the mobile data, BOYD storage data, cloud data and there is no concrete solution for data security, according to the 2010 data.

Breach Report from Verizon Business, 48% of breaches were caused by insiders, 90% of which were deliberate, and almost 50% of breaches involved privilege misuse [17], [18].

C. Provisioning

Provisioning refers to granting, managing access to an identity with maintaining confidentiality, integrity and availability. Provisioning in this classified with subgroup of security; IAM framework, standard, cloud based IAM. Burton Group Blogs [19], a research report projects that the IAM market will grow from nearly $2.6 billion in 2006 to more than $12.3 billion in 2014. As shown in (Table VI) 6% of all research articles contain information related to IAM solution. IAM solution provides auto-provisioning tools to reduce operational cost and reduce risk of security breach by eliminating redundant accounts and segregation of duties. For this review IAM solution has been put under the Taxonomy of the Provisioning, as the security domains are interrelated and difficult to separate it into an individual domain. Standards have been sub grouped into provisioning domain, as shown in (Table VI) 6% of article contained research on standards of IAM and organization. Combining the both subgroup give total of 12% articles researched in this area.

D. Compliance/Policy

Compliance domain classified with subgroup of policy, security awareness, workflow, as shown in (Table VI) information in the researched articles that has been reviewed for contains, policy 14%, compliance 8% workflow 6% compliance 8% and assurance 3%. Combining all three subgroup contain 41% of all material researched in the articles. It is also noted that in the year 2013 security

awareness has been researched most as in (Table V). This could be the reason of the on data breach and loss of data has emerged a new research to understand the underlying cause. In 2012 [5] survey of over 2,000 members of the UK public by Check Point and Yougov, over 50% of office workers said they regularly use unsafe working practices. 23% weren't aware of what their company's policy stated.

VI. Discussion

From the data analysis it has been found that 47% of all articles reviewed contained information related to the data security domain (Table VI), 41% of the information related to compliance and 12% information researched on IAM security solution. Looking into the subgroups of security, it shows that cloud computing 14%, security awareness 11%, policies 14% and compliance 8% of research content in the literature review. It can also be seen that in 2013 research (Table V) were published by both network security and computer fraud & security predominantly Security awareness, cloud security and policy based [20]. This could be linked to increase in level of cyber-crimes exploiting vulnerabilities the mobile devices. In 2012 first malware outbreak on Apple's OS X platform infecting an estimated 600000 machines stated [10]. According to survey carried out by PWC 45% of organization breaches security law, 75% of organization security policy have understood poorly, 54 is the median number for unauthorized outside threat on the organization [21]. Another survey carried out by Check Point and Yougov [5] on 2000 UK publics, it shows that 50% office worker carries out unsafe working practices that risk data breaches and loss ,e.g. forwarding critical information on personal e-mails, work e-mails on personal mobile devices, unencrypted data on USB sticks and on cloud. It has also been found that 23% of workers unaware what is the IT policy.

Issues with the data loss SME have realized too late [22]. This article emphasizes on data loss security policies rather than implementing expensive tool. Privacy compliance and legislation deals information life cycle management (ILM) to deal with the data workflow and loss. Recent issues with WikiLeaks incidence led to the user and regulator grapple with the issues, even the most secure organization are prone to security threat [23].

Cloud based IAM solution has gained popularity aligning with the information without the boundary theme. Traditional IAM access management system focused more on the in-house data provisioning. As technology evolving and more data hosted on the cloud and the mobile devices, it is becoming a challenge for organization to cope with the provisioning user access, combined with data protection legislation. From the data analysis it has been found that 6% of all information contain in the literature related to IAM solution. State of the art of IDM has been compared and concluded that "even after years of healthy adoption rates, the IDM market is actually just beginning its path toward broad adoption and deep penetration" [16].

Security in the cloud on the other hand perceived to be inherently less securing then a private network infrastructure. Concern with cloud being multi-tenanted, not knowing who ultimate service provider. Hybrid cloud computing is another new concepts [24], which provides private cloud for business critical and public cloud for least sensitive information. A new organization formed called open data center alliance (ODCA) for pushing tough security on cloud computing as the cloud is not doing enough to protect data and privacy. According to IAM solution have been implemented incorrectly up to date, business needs to rethink of the processes that require enhancement and not just plastering the process with a new robust tool [25], cloud based IAM has shown to possess security threat. Unrealistic optimism [26] in information security by the managers needs to be resolved. Simple cloud identity management (SCIM) provides a defined standard API and user schemas which has been adopted by vendors of cloud provider. [26] 8% of data security budget is spent on IAM research.

VII. Limitation and Future Work

Identity access management is a very critical in every sectors, government, financial, healthcare, retail, and defense. As the security functions are interrelated it has been difficult to group the function into a security taxonomy, however the security functions has been grouped in this systematic review based on the components of the IAM solution, data security, provisioning and compliance. Limitation within this exploratory systematic review as follow:

1) Search was conducted on various databases and search string may not have been words that may have been picked up other relevant articles.
2) Literature were limited to only English literature, there may have been other non-English literature that provided additional research conducted.
3) Literatures were search manually and prone to error, there might have been literatures which were eliminated in the initial identification phase.
4) Evaluation criteria used might not have been appropriate.

VIII. Conclusion

In the heart of IAM solution is the data security, it has been noted that nearly half of all the literature reviewed is data security related. Information on mobile devices and cloud possess threat and vulnerabilities, needs to be addressed. Mobile devices especially android have gained popularity and possess vulnerabilities. Data accessed and transferred to personal mobile devices should be encrypted. It has also been highlighted flaws in security policies poorly understood, lacking in security awareness, security best practices. Security data flow will need to be documented and unrealistic optimism of information security from the management will need to be resolved. Organization will need to comply with data security legislation and standards and have data loss handling process in place.

IAM solution is still being researched and has not been adopted effectively; however it has obtained attention from wider market. Cloud based IAM which shown to provide some degree of flexibility coping with deparametised organization however it has shown to possess security weaknesses. Open data center alliance (ODCA) for pushing tough security on cloud computing. Perhaps organization will

need to plan out their critical service through service risk assessment collaborating with the business stakeholder and well as the IT to plan out a road map of what is that require to secure information , maintaining the confidentiality, Integrity and availability.

Based on the evidence to conclude on research question three; least researched IAM taxonomy is the provisioning, As the IAM technology solution is still evolving and new mobile technology proving to be a challenge. Research questions two; what IAM security functionality being address in the development of IAM? Auto-provision, operational efficiencies, cost reduction, segregation of duties, role management and compliance legislation. Question one; Research activities on framework / model and best practices for IAM? Recent years it has been cloud based security (hybrid solution), previously focused more in-house infrastructure, role model engineering (rbac, tbac) , weakness and strength of various IAM solutions, new wave of IAM solution to rectify the previous IAM implementation. Lastly technology alone will not be enough to make organization secure it is the people, process and the IT that need to work coherently to make a secure information system. Future research is to fill the gap between the organization information flow security requirements and aligning it with the IAM solution.

ACKNOWLEDGMENT

Knowledge and expertise of IAM and security has been gained through commercial experience within investment Banking used to compare literature review with real world issues.

REFERENCES

[1] C. Tracey, "Security at the data level," *Network Security*, issue 5, pp. 6-12, May 2013.
[2] C. Everett, "Identity and Access management: the second wave," *Computer Fraud & Security*, issue 5, pp. 11-13, May 2011.
[3] M. S. Ferdous and R. Poet, "A comparative analysis of identity management systems," in *Proc. 2012 International Conference on High Performance Computing and Simulation*, 2012, pp. 454-461.
[4] G. Vrhovec, "Beating the privacy challenge," *Computer Fraud & Security*, issue 3, pp. 5-8, 2011.
[5] C. Tracey, "Identity — The new parameter," *Network Security*, issue 4, pp. 14-18, April 2013.
[6] S. Tessier, "From management controls to the management of controls accounting," *Auditing & Accountability Journal*, vol. 25, no. 5, pp. 776-805, 2005.
[7] A. Liberati, D. G. Altman, J. Tetzlaff, C. Mulrow, P. C.Gøtzsche, J. P. A. Ioannidis *et al*., "The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration," *JClin Epidemiol* 2009; 62(10):e1–34.
[8] H.-S. Rhee, U. R. Young, and C.-T. Kim, "Unrealistic optimism on information security management," *Computers & Security*, vol. 31, issue 2, pp. 221-232, 2012.
[9] S. J. Alotaibi and M. Wald, "IAMS framework: A new framework for acceptable user experiences for integrating physical and virtual identity access management systems internet security," (WorldCIS), World Congress on, pp. 17–22, 2012.
[10] S. Mansfield-Devine, "Security review: The past year," *Computer Fraud & Security*, 2013.
[11] M. Potts, "The state of information security," *Network Security*, vol. 2012, issue 7, pp. 9-11.
[12] S. Travis, "Identity in the cloud, computer," *Fraud & Security*, issue 7, pp. 19-20, July 2012.
[13] D. Shlomi, "Privileged identity management: Securing the enterprise Network," *Security*, vol. 2010, issue 12, pp. 4-6, December 2010.
[14] H. Jason, "Why the traditional approach to information security is no longer working," *Network Security*, issue 1, pp. 12-14, 2013.
[15] In brief, *Network Security*, issue 3, p. 3, 2011.
[16] K. S. Madhan and R. Paul, "A roadmap for the comparison of identity management solutions based on state-of-the-art IDM Taxonomies," *Education & Research*, Mysore, India: Infosys Technologies, 2010.
[17] L. Fuchs, G. Pernul, and R. Sandhu, "Roles in information security — A survey and classification of the research area," *Computers & Security*, vol. 30, issue 8, pp. 748-769, 2011.
[18] Lewis Nick, "Access rights — Protect access to your data or lose it: Serious misconceptions about information security," *Computer Fraud & Security*, vol. 2012, issue 11, pp. 8-10, Nov. 2012.
[19] Burton Group Blogs. Identity and privacy. [Online]. Available: http://identityblog.burtongroup.com/bgidps
[20] B. Guy, "Technology is not enough: Taking a holistic view for information assurance," *Information Security Technical Report*, vol. 17, pp. 19-25, 2012.
[21] Information security breaches survey: Technical report PWC. (April 2012). [Online]. Available: http://www.pwc.co.uk/en_uk/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf
[22] P. Stephen, "Black hole business security," *Info Security*, 2010.
[23] D. Steve, "Information security without boundaries," *Network Security*, vol. 2011, issue 2, pp. 4-8, 2011.
[24] B. Richard, "Information security in the cloud," *Network Security*, issue 4, pp. 15-17, 2011.
[25] P. G. Dorey and A. Leite "Commentary: Cloud computing a security problem or solution?" *Information Security Technical Report*, vol. 16, issue 3–4, pp. 89-96, August–November 2011.
[26] M. Courtney, "Who, what, why, where — And when," *Engineering and Technology*, vol. 6, issue 6, pp. 38–40, 2011.

Mumina Uddin was born in Sylhet, Bangladesh. She was living in UK since childhood. She completed her BSc (hons) degree in biomedical sciences and the MSC (hons) degree in information systems from Brunel University. She had worked 13 years as an information security consultant within the big four Investment Banks in London and perusing research in identity access management solution.