A Survey on Ciphertext-Policy Attribute-based Encryption (CP-ABE) Approaches to Data Security on Mobile Devices and its Application to IoT

Steve Moffat
Manchester Metropolitan University
stephen.moffat@stu.mmu.ac.uk

Dr. Mohammad Hammoudeh
Manchester Metropolitan University
m.hammoudeh@mmu.ac.uk

Dr. Robert Hegarty
Manchester Metropolitan University
r.hegarty@mmu.ac.uk

ABSTRACT

The growth in Cloud Computing and the ubiquity of Mobile devices to access Cloud services has generated a new paradigm, Mobile Cloud Computing (MCC). While the benefits of storing and accessing data in the Cloud are well documented there are concerns relating to the security of such data through data corruption, theft, exploitation or deletion. Innovative encryption schemes have been developed to address the challenges of data protection in the Cloud and having greater control over who should be accessing what data, one of which is Attribute-Based Encryption (ABE). ABE is a type of role-based access control encryption solution which allows data owners and data consumers or users to encrypt and decrypt based on their personal attributes (e.g. department, location, gender, role). A number of ABE schemes have been developed over the years but ABE in MCC has established its own paradigm driven by a) the use of mobile devices to access private data hosted in the Cloud and b) the physical limitations of the mobile device to perform complex computation in support of encryption and decryption in ABE. ABE in MCC is an evolving research field but given the breadth and strength of interest at time of writing it is timely to perform a survey. Due to the sheer volume of research, the survey has focused on one aspect of ABE - Ciphertext-Policy Attribute-Based Encryption - in line with its prominence in ABE in MCC research to date. Further, given the significant developments and interest in IoT, the survey has since been extended to assess whether the research into mobile devices has been translated to the application of attribute-based encryption in IoT where the challenges to support complex computation and data transmission are potentially more complex given the much greater heterogeneity and resource restrictions of IoT devices.

CCS CONCEPTS

•Security and privacy → Key management; Access control; Mobile and wireless security; *Public key encryption; Block and stream ciphers; Authorization; Usability in security and privacy;* **•Networks → Cloud computing; Public Internet;** *Wireless access networks; Wireless personal area networks;*

KEYWORDS

Ciphertext-Policy Attribute-Based Encryption, CP-ABE, Mobile device, Mobile Cloud Computing, MCC, IoT

1 INTRODUCTION

With the rapid development of Cloud computing technology and services there has been a surge in individuals, groups and organisations uploading data into the Cloud for ease of use or cost-saving. Included in this data are the highly sensitive and there are growing concerns relating to the security and privacy of such data. Examples of accidental or intentional access to private data by Cloud service provider employees, distribution of sensitive data by individuals through accident or ignorance as well as 3rd parties with criminal or malicious intent to exploit exposure of private data are ever-present in today's digital world.

The challenges of data security (integrity and confidentiality) have been addressed to some extent through the adoption of encryption methods for data *in situ* (on the device or Cloud infrastructure) and *in transit* across the network. However, such schemes are limited due to the significant overhead of administering encryption keys for a multitude of data types, files or documents, to a wide range of individuals or groups. One of the key weaknesses of such schemes is unauthorised access through collusion. In this situation users will be able to share keys to gain access beyond their rights.

In parallel with the growth in Cloud Computing has been the extensive use of mobile devices and associated applications to access Cloud services, establishing its own paradigm, Mobile Cloud Computing (MCC). Such a scenario has generated significant research into data security in MCC. In particular, there have been a number of recent developments in secure fine-grained access control systems based on Attribute-based encryption (ABE).

The application of ABE in MCC raises new challenges due to ABE's dependency on complex computation in support of encryption and decryption and the physical constraints of mobile devices (process, battery, bandwidth). Since 2015 the volume of research into ABE in MCC has increased significantly.

The first part of the survey focuses on Ciphertext-Policy ABE (CP-ABE)in MCC primarily due to the fact that most ABE schemes in MCC appear to be based on CP-ABE or extensions to it. The second part of the paper is to assess the research into the application of ABE in IoT and determine whether the schemes from CP-ABE in MCC have been translated as potentially applicable - either directly or with some minor enhancements - to data security in IoT. The approach is to describe the schemes' system architectures using consistent notation and terminologies where appropriate and then measure each in terms of performance and security.

2 RELATED WORKS

ABE was first proposed by Sahai and Waters [1] and was considered a promising cryptographic technique in support of data confidentiality and access control simultaneously. Its emphasis was on *Identity*-Based Encryption where an identity was viewed as a set of attributes. In the paper they stated a private key for an identity with attributes *w* could only decrypt a ciphertext encrypted with an identity *w'* if and only if the identities (i.e. the attributes) sufficiently matched.A crucial security aspect of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. ABE has now spawned a number of schemes, each of which have generated schemes addressing a wide range of access control problems. For example, Goyal and Sahai [2] extended the ABE scheme to deliver a fine-grained access control system. In their scheme each ciphertext is labeled by the encryptor with a set of descriptive attributes. Each private key is associated with an access structure that specifies which type of ciphertexts the key can decrypt. This they defined as Key-Policy Attribute-based Encryption (KP-ABE). Bethancourt et al [3] developed an alternative ABE scheme, Ciphertext-Policy Attribute Based Encryption (CP-ABE). In their system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, the methods are conceptually closer to traditional access control methods such as role-based access control (RBAC). Several ABE schemes have developed in recent years. Kumar et al [4] classified ABE as shown in Figure 1.

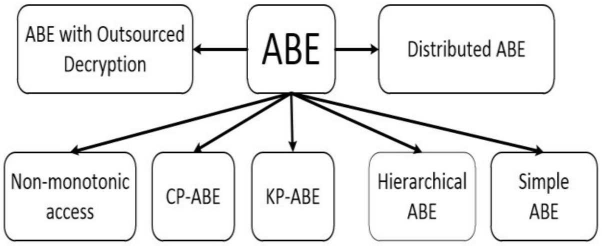

Figure 1: ABE Classification (Kumar et al [4])

As shown above, there are other examples of ABE but KP-ABE and CP-ABE have become the most prominent. The breadth of research across these areas is wide and increasing therefore the survey has aimed to target the ABE scheme which is most prominent in Mobile Cloud Computing. Research supporting the survey indicates that the ABE in MCC is led by CP-ABE.

A survey of ABE was performed by Qaio et al [5] in 2014 but there does not appear to be an equivalent for ABE in MCC. This may be due to the fact ABE in MCC is a recent area of research and as such researchers are awaiting further developments before considering whether a survey at this stage will be of value.

3 A BRIEF OVERVIEW OF CP-ABE

Scenario: A Data Owner wishes to share private data with a number of Data Users. Assume the data is stored in the Cloud. Rather than provide access to the data individually the Data Owner will allow Data Users to have access to the data if and only if a Data User has the appropriate credentials which in this case are the right set of attributes. The Data Owner applies an *Access Policy* to the private data. If the Data User's attributes meet the access policy then the Data User may access the data. See Figure 2.

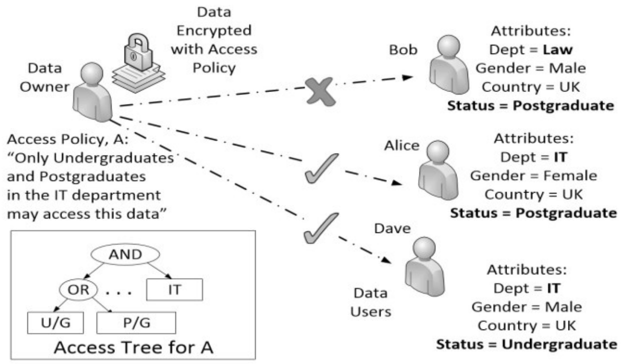

Figure 2: A functional overview of CP-ABE

CP-ABE meets this requirement by a) the Data Owner encapsulating the access policy and data in a single Ciphertext and b) the Data User decrypts the ciphertext using their secret key if and only if they have the appropriate attributes. The implementation of CP-ABE is based on four algorithms: (i) Set-up (ii) Key Generation, (iii) Encryption, (iv) Decryption ((v) Global set-up)

3.1 The CP-ABE Algorithms

Notation	Description
DO	Data Owner
DU	Data User
CS	Cloud Server
AA	Attribute Authority
PK	Public Key
MK	Master Key
SK	Secret Key
A	Access Set/Access Policy
AU	Attribute Universe
w	Attribute Set
M	Unencrypted Message
CT	Ciphertext of Message
E/Enc	Encryption function

Table 1: Notation and Terminologies

An Attribute Universe, AU, is the total set of attributes of a user population. In CP-ABE, when a Data Owner, DO, configures an access set, A, for his data, M, it is based on the combination of a set of attributes taken from the AU. The DO encrypts both the message, M and its associated access set, A, through a public key, PK. A Data User, DU, is assigned a private key, SK, which is associated with his attribute list - also a subset of the AU. The PK and SK have both been generated from the same Master Key by the AA. The DU can decrypt the message with SK if and only if the the attribute list associated with SK meet the criteria of the access set for that message.

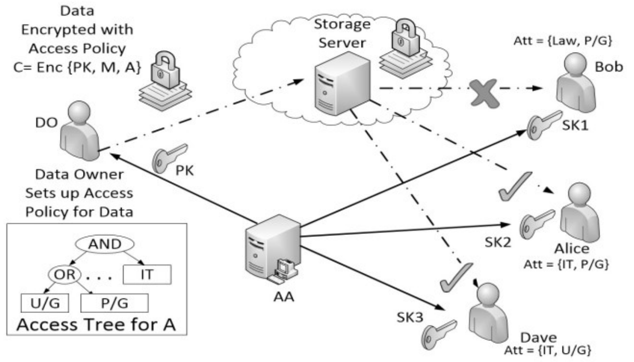

Figure 3: CP-ABE Implementation

(1) Setup: The Setup algorithm takes as input a security parameter, and returns the public key PK as well as a system master secret key MK. PK is used by the DO for encryption. The AA will use the MK to generate secret keys, SK for the Data Users. The MK is known only to the key authority. Setup:$\{\lambda\}\rightarrow\{MK, PK\}$

(2) Encrypt: This algorithm takes as input the PK, a plaintext message M, and an access structure A. It outputs the ciphertext CT.
Enc:$\{PK, MK, A\}\rightarrow CT$

(3) Key-Generation: This algorithm takes as input a set of attributes w, associated with the user and the master secret key, MK. It outputs a secret key SK. KeyGen:$\{MK, w\}\rightarrow SK$

(4) Decrypt: This algorithm takes as input the ciphertext CT and a secret key SK for an attribute set. It returns the message M if and only if the attribute set satisfies the access structure associated with the ciphertext CT.
Dec:$\{SK, CT\}\rightarrow M$

4 CP-ABE IN MOBILE CLOUD COMPUTING ARCHITECTURE

4.1 The Challenges of CP-ABE in MCC

Having described the algorithms which comprise CP-ABE it is appropriate to describe the challenges which need to be addressed in CP-ABE.

The three major technical challenges for the end user, the DO and the DU, are:

(1) (DO) Ciphertext Computation Cost: As the access policy increases in complexity, the levels of bilinear pairing and exponentiation operations also increases, resulting in computation costs increasing. Such calculations have a major impact on performance when executed on mobile and IoT devices

(2) (DO) Ciphertext Communication Cost: As well as the computation cost, CP-ABE ciphertext constructions are very large as the access policy increases. Sending such messages over MCC and IoT bandwidth leads to a significant communication cost.

(3) (DU) Secret Key Computation Cost: The impact of decryption of the ciphertext on the recipient mobile or IoT device is also a major consideration particularly when the size of the ciphertext becomes extensive.

Each of the schemes considered in this review aim to tackle these challenges in different ways.

4.2 Architecture features

The schemes researched to date have developed different architectures to address the problem of resource-constrained mobile devices. The following list aims to provide a summary of the architectural features which dictate the schemes. Note that some schemes may use a combination of these features. Architecture features:

(1) **Encryption in the Cloud:** ABE encryption is delegated from the mobile device to the Cloud server
(2) **Decryption in the Cloud:** ABE decryption is delegated from the mobile device to the Cloud server
(3) **Pre-encryption:** ABE encryption is de-constructed into pre-encryption and then encryption to distribute computation costs
(4) **Pre-decryption:** ABE decryption is de-constructed into pre-decryption and then decryption to distribute computation costs
(5) **Constant-size ciphertexts:** Limiting the computation impact of extensive attribute lists defining the access policy through constant-size ciphertexts
(6) **Constant-size secret keys:** limiting the computation impact of extensive attribute sets of individuals through constant-size secret keys
(7) **Multiple Authority extension:** where the CPABE scheme operates across multiple attribute authorities which combined support a large scale "universal attribute set"
(8) **Online-Offline feature:**Where ABE encryption or decryption in the scheme is not wholly dependent on Cloud services. The Offline feature is where the mobile device while not being connected to the internet is able to perform higher levels of local complex computation while connected to a mains (i.e. during charging).

4.3 CP-ABE for MCC Capabilities: Scheme Assessment Criteria

(1) **Performance:** Does the scheme degrade as it scales up? Does it deliver fast encryption and/or decryption? Are there minimum device configurations or requirements? Is the system architecture robust and delivers consistent performance? What are the computational costs?
(2) **Security:** Is the security of the scheme robust or has the efficiency of the scheme compromised the level of security or access control?

A note on Revocation: Each scheme was to be assessed on its ability to manage revocation of keys. That is to say, does the scheme's design add complexity or simplify key revocation? Having reviewed the schemes and CP-ABE generally revocation is an inherent problem for such large-scale systems and is a research area in its own right. It will therefore not be one of the assessment criteria.

5 CP-ABE SCHEMES IN MCC

5.1 ABE Encryption and Decryption in the Cloud

To address the challenges of mobile device constraints to perform complex encryption and decryption Jin et al [6] have proposed a scheme - Secure and Lightweight CP-ABE (SLCP-ABE). In this scheme the heavy computational tasks are outsourced to the Encryption Proxy Server (EPS) and Decryption Proxy Server (DPS) located in the Cloud as described in the system architecture in Figure 4.

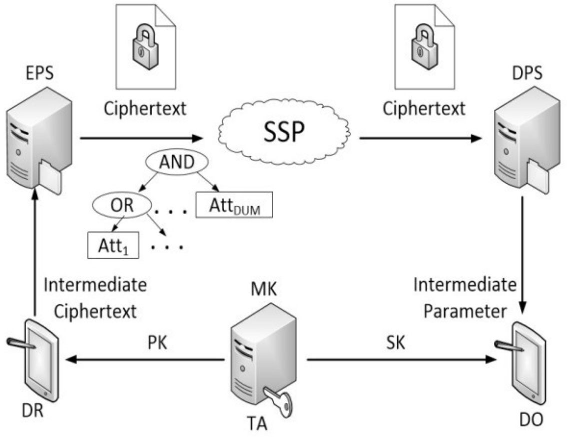

Figure 4: CP-ABE Encryption and Decryption (Jin et al [6])

During running of the Setup algorithm the TA generates the *PK* and *MK* according to the attribute database. Jin et al introduce the addition of a *dummy* attribute to each user's attribute set. The TA then runs the Keygen algorithm to create a user's secret key, *SK*, which is associated with her attribute set (including the dummy attribute) according to *MK*. The Encryption is then broken down into two levels of encryption computation: light (Encryption A) and heavy (Encryption B). During Encryption A, Jin et al propose that the Data Owner uses the mobile device to generate an *intermediate* Ciphertext *CTI* which is an encryption of the access tree *and the dummy attribute* and the message based on the private key, *PK*. The *DO* then sends *CTI* to the Encryption Proxy Service, EPS. Encryption B performs the computationally intensive exponentiation associated with the encryption and generates a single ciphertext which encapsulates the access set and the message and sends to the CSP. During Decryption, the DU requests the CT from the CSP. The CSP checks the DU's attribute set meet the access tree. If so, the CSP sends the CT to the DPS. Further authentication of the user based on their set and supported by SK is performed by the DPS. If successful, an intermediate parameter is sent to the DU by the DPS, who is then able to run the decryption algorithm to obtain the message.

Performance The concept of moving heavy computation to proxy servers is an interesting one and the evidence from tests show the significant improvements over mobile devices. As with any addition of services and infrastructure to a scheme the question of performance degradation relative to direct integration between mobile device and CPS needs assessment. Jin et al provide evidence of the level of performance between the servers and the mobile devices and as expected the servers perform extremely well. There is however no reference to the impact of sending data over an extra hop to get to CSP relative to direct communication between mobile and CSP. The argument may be that such a discussion is unwarranted since such transmissions do not necessarily have to be in real time. As long as the encrypted data and its associated access list reach the CSP in an acceptable time then this will suffice. If that is the assumption then it needs to be made clear. On the Decryption side such an argument may not hold. On the one hand the user appreciates that the request to gain access has been broken down into two transactions and the frustration of mobile device performance is removed. On the other hand there is no understanding of the impact of relying on 2 services from a response time perspective. Additionally, the reliability of the architecture may be questioned due to the dependency on additional services and servers, EPS and DPS. Operationally, the EPS and DPS are likely to be hosted either on premise or at another infrastructure CSP. *Security* Evaluating the security analysis by Jin et al, is is very comprehensive in that it covers each aspect of data confidentiality, fine-grained access control is in line with standard CP-ABE solutions. They also refer to user access privilege but even though the Cloud servers can obtain subsets of the attribute sets of users there is no risk of gaining the full attribute set. What is not clearly explained is what risks there are regarding access to a subset of attributes. Collusion - the sharing of keys between Data Users to gain access to a wider data set - is identified as a core property of CP-ABE.

5.2 On-line/Off-line encryption

Proposals for online/offline schemes in the field of CP-ABE were first submitted by Hohenburger and Waters [7]. The computational cost of ABE to perform ciphertext encryption and key generation as access policy complexity or number of user attributes increased were well understood. Rather than just accept poor performance on the device or identify ways of moving the computation to servers they proposed a scheme where “a mobile device could be programmed to automatically do ABE preparation whenever it is plugged into a power source, and then when it is unplugged, ABE ciphertexts could be rapidly formed with a significant reduction in battery consumption”. The concept is similar to the encryption/decryption scheme described earlier in that an intermediate ciphertext is created on the mobile device but the extent of its encryption is greater when the device is working offline and then directly sends to the CSP when on-line. In [7] Hohenburger and Waters focused on the Encryption phase and in particular the “preparation phase” performed on the mobile device offline, a significant amount of the work to encrypt the message OR create a key *before* it knows the access control policy. Once the details of the access policy are known then the ABE ciphertext can be rapidly constructed. As can be seen in the following schemes Online/Offline has been adopted into wider schemes such as Pre-decryption and Pre-encryption as well as multiauthority schemes.

5.3 Pre-encryption and Pre-decryption and Anonymous CP-ABE

One of the concerns relating to ABE is the set of attributes may help determine who is the target receiver which exposes the user’s privacy. By knowing the user’s identity it may be possible to know the nature of the plaintext. To tackle this problem *anonymous* ABE schemes have developed over the years. In *anonymous CP-ABE* the recipient aims to decrypt using the secret key with the appropriate attribute set for that access policy. The problem arises when the user is rejected because he has supplied the wrong key. Under anonymous CP-ABE, Zhang et al [8] identified that one of the major problems for users was not knowing which key should be used during decryption and a user may have several keys (for different messages and access policies) and keep trying before succeeding. In MCC this puts a significant overhead on the the mobile device. Their scheme introduced a new technique called “match-then-decrypt”. In such a scheme special components of the ciphertext are used to test the access policy against the attributes in the private key without performing decryption. If there is a match then decryption will take place. Zhang et al[9] have recently proposed a scheme to improve the encryption process for anonymous CP-ABE by “introducing a match-then-re-encrypt technique which they call CP-ABPRE (see Figure 5 for the system architecture).

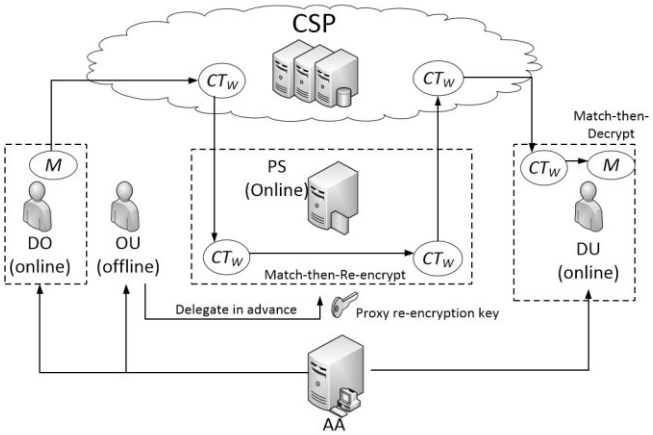

Figure 5: Proxy re-encryption and Anon. CP-ABE (Zhang et al [9])

Similar to the aforementioned match-then-decrypt technique, “this technique works by computing special components in proxy re-encryption keys and ciphertexts which are used to check whether the proxy can fulfill a proxy re-encryption or not”. On successful re-encryption the scheme extends to the match-then-decrypt technique to offer an all-round preencryption, pre-decryption solution.

Performance In Figures 6 and 7 Zhang et al [9] provide evidence to show the improvements made by pre-decryption and pre-encryption.

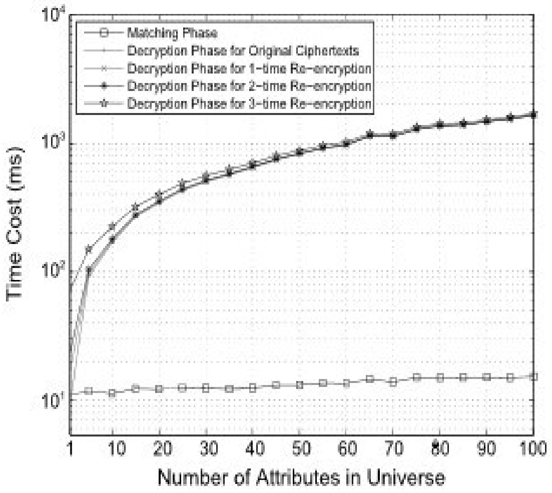

Figure 6: Decryption cost for anonymous CPABPRE. (Zhang et al [9])

Performance In Figures 6 and 7 below Zhang et al provide evidence to show the improvements made by pre-decryption. This is supplemented in the later paper on re-encryption.

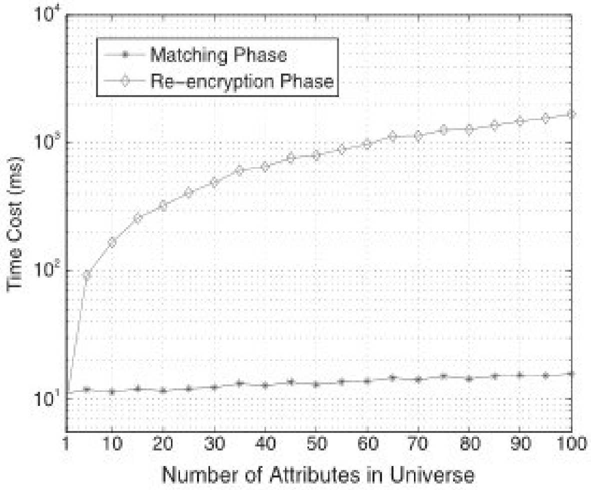

Figure 7: Re-encryption cost for anonymous CPABPRE. (Zhang et al [9])

5.4 Constant-size ciphertexts and Constant-size secret keys

As has been stated, computational complexity and costs to encrypt and decrypt the ciphertext puts significant burden on the mobile device of the data owner and data user respectively. While there are significant developments in the areas of pre-encryption, outsourcing of encryption and decryption to reduce the impact on the devices, Chen et al [10] developed a scheme to limit the level of computation irrespective of the access structure complexity. Zhang et al [11] have extended Chen et al's scheme to deliver small computation costs and constant-size ciphertexts.

Another challenge is the computation of secret keys. The size of secret keys can also be extended as the size of the Data User's attribute list increases. As users access a wider range of services their attribute list increases to meet the requirements of a wider range of access policies. This will put increasing demands on the mobile device to decrypt. Guo et al [12] proposed a CP-ABE scheme with constant-size secret keys. In the scheme Guo et al make two major contributions in their paper. The first is to deliver a constant-size Security Key irrespective of the size of attribute list but the other is to apply this to very lightweight devices as the decryption key can be a small as 672-bits. Its applications are potentially wide-ranging.

Odelu et al [13] have recently taken the discussion further in delivering a scheme which delivers both constant-size ciphertexts and security keys. identified that while both improved the efficiency of encryption and decryption and potentially offered improvements to the

Performance The benefits of constant-size ciphertexts and secret keys are obvious. Any schemes which limit the impact on a mobile device's performance to encrypt or decrypt irrespective of the complexity of the access policy or size of the attribute list are a useful addition to the portfolio of options. As data owners share more of their data to a wider audience or users wish to access more services and data sources such schemes will ensure performance is not hindered. Odelu et al do provide evidence of the performance improvement in the their scheme over others based on the sizes of the security key and the ciphertext generated. The sizing is based on pairing groups and length of plaintext. At this point in time it is beyond this author's knowledge to understand how the scheme compares relative to others in the table provided by Odelu et al. Suffice to say that based on the variables provided the scheme delivers constant-size ciphertexts and secret keys at sizes which are of lower order than other schemes (multiples of bilinear group or plaintext message size)

5.5 Multi-Authority Extensions

The schemes discussed in this survey thus far are based to a large extent on a single Attribute Authority in the assignment of keys in support of access policies of the data owner or the attribute set of the data user. One of the biggest concerns with standard ABE schemes is the exposure of risk to of a single attribute authority. The AA has full visibility of access structures and attribute lists. If the attributes were distributed across multiple authorities then the risk is somewhat reduced. Furthermore, thee is a recognition that in "real world" conditions the likelihood is that multiple authorities may participate in the maintenance and distribution of such keys. In order for this to operate effectively then additional services are required to minimise the Data Owner and Data User being inundated with a number of keys to maintain the appropriate level of security. It is worthwhile explaining the concept of Multi-authority schemes. In such a scheme assume there are multiple attribute authorities each of which has its own attribute universe for a group of users. The Data Owner is aware that no single authority is able to support their access policy as the AA will only generate keys for a subset of such attributes. In order for the AA's to operate effectively additional parties are added to the implementation of the scheme to maintain unique identities and keys which "unify" the local private keys and secret keys from the individual Attribute Authorities. At one time proposed multi-authority ABE schemes had been limited by the fact that once the PK had been set up then there was no flexibility in the schemes to accommodate access structure or attribute changes. Li et al [14] proposed a provable secure *unbounded* multi-authority CPABE scheme. The standard CP-ABE scheme is extended to accommodate Global service providers. The *Global* Set-up algorithm generates Global PK's - effectively managing the uniqueness of ALL users in the system. A Central Authority then generates its own MK and PK (similar to a single authority schemes described earlier) using the Global PK as input. The AA's meanwhile, which individually support a subset of the attribute set supporting the system, generate their own MK, PK and SK for the attributes they support. It is the role of the CA to generate identity keys which links all the attribute keys to a user's GID. It is this unique key which drives the encryption and decryption process.

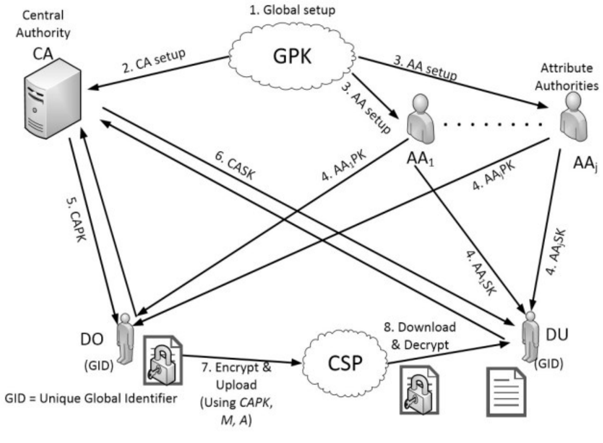

Figure 8: Multi-authority CP-ABE (Li et al [14])

Zhang et al[15] have extended Li's solution by introducing Offline-Online attribute-based encryption. In this scheme the secret key generation and encryption are both performed off-line. The recommendation is that "the Global Identity and Attribute Authorities can each issue secret keys before knowing the GID and attributes. The DO can perform encryption computation before knowing the the actual message or and access structure".

The system architecture of Zhang et al's is shown below.

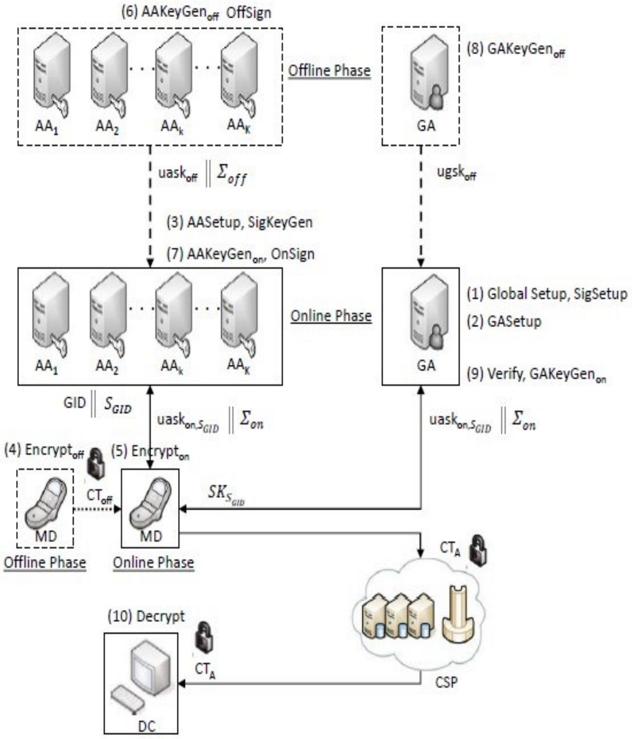

Figure 9: System architecture of online/offline multi-authority attribute-based data sharing system (Zhang et al [15])

Performance Looking at the evidence from Zhang's paper it is clear that there are significant improvements to be gained when applying online/offline techniques to Li's original scheme (see Figure 2 in Zhang et al[15] - Online computation cost comparisons between fully large universe constructions). Where this diverges from other online/offline schemes is that it brings into play the service providers (Global and Attribute Authorities) operating offline. However, if the multi-authority model is the way forward then it will be incumbent on these organisations to offer the optimum service. One major concern is the operational aspect of multiple authorities supporting the system. Although the authorities operate independently in this scheme the more participants supporting such a scheme the grater the risk in potential failures in the system.

Security Although there are a number of actors throughout the scheme the primary objective of multi-authority schemes is to address security by ensuring no single Attribute Authority holds all the information relating to access policies or attributes.

6 THE APPLICATION OF CP-ABE TO THE INTERNET OF THINGS

Following the survey of CP-ABE in MCC the paper has been extended to identify whether such schemes have generated further research in their application to "lighter" devices in the IoT. The following schemes are some of those identified to date.

Yao et al. [16] propose a lightweight ABE scheme for IoT which is based on elliptic curve cryptography (ECDDH) for security rather than bilinear pairing to improve efficiency and reduce the computational and communication overhead. Evaluating its performance against other schemes - both KPABE and CP-ABE - the computation improvements are significant. The authors highlight the limitations of the scheme in terms of: inflexibility of attribute revocation - a generic problem with most ABE schemes - but there will be future work to investigate this; poor scalability in that as as attributes are increased the computational and communication overhead increases linearly - similar to a number of ABE schemes unless adopting constant-size ciphertext and secret key solutions; poor generality in that the scheme has been tested against Unit IoT (single authority or domain application) rather than ubiquitous IoT (cross domain).

Further research into both its scalability and generality are required.

The scheme proposed by Touati et al [18] - Cooperative CP ABE (C-CB-ABE) - aligns with some of the schemes from MCC based on the principle of delegating the heavy computation and communication to more powerful devices which Touati et al refer to as "assisting nodes".

Evaluating the performance, Touati et al confirm that the actual computation is exactly the same but by distributing it to the more powerful assistant nodes performance significantly improves. The communication cost in terms of energy expended to send from to the assistant nodes is less than the energy saved in delegating the computation.

The scheme is also secure in that all communication between the device and assistant node is secure. Further, the storage server is unable to recover the original message due to the partial encryption performed across the device and node.

Recommendations on the number of assistant nodes is provided (n = 5) which will gain thew correct balance between robustness and efficiency. [Further information providing a simple formula to calculate the optimum assistant node configuration based on number of devices, complexity of encryption and frequency of encryption (transmissions between device and node) would be useful].

As well as Co-operative CP-ABE Touati et al [20] propose a scheme to enhance the efficiency of CP-ABE Attribute and Key management. It is recognised that attribute revocation is a general problem in CP-ABE due to the nature of regenerating a significant number of keys and/or re-assignment of attributes to all users. Given the heterogeneity of devices, the volume of devices and the breadth of applications and the rate at which such factors are increasing then revocation could become a major concern in the adoption and application of CP-ABE to IoT.

In their paper, Touati et al base their scheme on the premise that attributes are known in advance and that the response to change can be managed by a combination of good planning and the application of time periods when the attribute/s is/are valid. They reason that for large institutions such as health and education then such planning is perfectly feasible. This then means the keys associated with a user's attributes no longer need to be re-issued in response to change but instead the decryption algorithm checks the validity of the attribute based on time.

It is clear that such a scheme could be beneficial under the appropriate conditions that is, not only in terms of low volatility but in the planning of how such change is applied in advance with the attribute authority. Applying this to a wider context such as Multi-Authority, will be more complex but more at the administrative level as opposed to technical. The survey thus far has focused on individual schemes which aim to overcome the challenges of ABE - and, in particular, CP-ABE - due to the limitations of Mobile and IoT devices. Though not a specific scheme, Ambrosin et al [21] have performed a study of ABE on IoT devices building on their similar investigation into the feasibility of ABE on Smartphone devices [22]. The paper provides a summary of performance (execution time), memory and energy consumption in relation to processor (intel and Raspberry Pi), number of attributes and levels of encryption (80-, 112- and 128-bit). The paper also provides an application example in healthcare for the collation of data from a number of sensors generating ECG data and securely sending to a central server.

The conclusions from the paper are that with appropriate memory management, customised data structure deployment and simplified cryptographic arithmetic operations there is strong potential in ABE (both KP- and CP-) in its application to IoT. Further, the complex arithmetic operations could potentially move to hardware accelerators which to some extent aligns neatly with C-CP-ABE referenced above.

7 FINDINGS

In recent years there has been significant growth in the adoption of mobile devices, mobile applications and Cloud services and this is likely to continue for a number of years. Their adoption has resulted in the increasing risk of exposure of data in various sectors spanning personal (health, financial, social), corporate (intellectual property, financial, commercial) and public (e.g. health services, education, crime prevention). CP-ABE has been identified as one approach to addressing some of the challenges of data security on Mobile devices and Mobile Cloud Computing generally.

Based on the research reviewed in this survey, the general view is that the computational demands of CP-ABE encryption and decryption is inefficient on Mobile devices due to their physical limitations: processor and battery power as well as network bandwidth. To address these constraints several creative schemes have been proposed.

(1) Developments in more efficient attribute-based encryption algorithms will reduce the levels of computation which has the potential of making it more ubiquitous across a wider range of devices.
(2) The distribution of computation across mobile devices and dedicated encryption-decryption proxy servers offers further potential but this brings with it a more complex operating model spanning device-encryption proxy server-host architecture.
(3) The Offline-Online architecture also provides opportunities but this must be weighed against the impact of encryption/decryption being a two-phase and not real-time transaction.
(4) Fixed-size ciphertext and security key schemes are a move towards computation optimisation such that increasing levels of complexity in access rules or attributes will have minimal impact on encryption/decryption computation.
(5) Most schemes are based on the single attribute-authority scenario. In reality there may be several attribute authorities and proposed schemes are evolving in this area. The challenge will be the operational aspect of coordinating a multitude of attribute authorities.

A review of the application of attribute-based encryption schemes to IoT suggest that it is developing its own paradigm and that there is little that has been translated from the CPABE in MCC to IoT. The key findings are as follows:

(1) Increasing the efficiency and reducing the complexity of encryption-generated computation will be a significant benefit in IoT but such schemes used for MCC do not appear to be transferable to IoT at this stage and IoT may have to develop its own schemes such as the one developed by Yao et al.
(2) Delegation of encryption to trusted "assistant nodes" which exist on the same network as the IoT device but are able to perform heavier computation and data transmissions. Similar to the proxy servers identified in the MCC schemes it is assumed their operational management will be significantly simpler being on the same local network as the IoT devices. Potential performance and scalability benefits are envisaged. If assistant nodes could also operate as surrogate firewalls then security benefits may also be realised but this will need to be weighed against the impact on performance.
(3) The research into performance of lightweight devices by Ambrosin et al is an area which appears to be growing generally. Their findings suggest that lightweight devices could potentially support CP-ABE however further investigation into memory, processor, battery and network capacities is required. Such research could be consolidated to develop a model of device sizing against computation (encryption at bit and attribute level) and performance. More empirical evidence of CP-ABE across a wider range of IoT devices using the methodology described would be of great value.

8 CONCLUSION

CP-ABE is an extremely useful scheme to address the risks associated with data security in the Cloud. It provides a certain level of flexibility and scalability in that it removes the need for data owners to manage every individual request. Instead, the data owner maintains an access policy and if the user has the appropriate attributes then she will gain access. This survey's objectives were to describe how the inherent computation complexity and communication costs of CP-ABE are a major concern in MCC and IoT and may hinder its adoption. The survey has also identified that there are a number of creative schemes to address these concerns including offline/online algorithms, computation delegation through proxy server processing, computationand communication-limiting schemes using constantsize ciphertexts and security keys and risk-management and scalable solutions identified in multi-authority schemes.

CP-ABE in MCC is still a relatively new area of research and it is likely to grow significantly in line with the growth in MCC and users wanting access to increasing amounts of data and services on the one hand and on the other the increasing concerns of individuals, groups, corporations and governments regarding the security of their private data.

The application of ABE, and CP-ABE in particular, to IoT is generating its own paradigm. While some research in this area is based on previous mobile device research (Ambrosin et al) there does not appear to be a significant amount from Mobile device schemes being applied to the IoT at this stage. There is general consensus that computation needs to be more efficient on the one hand and hardware and network improvements on the other to see real benefits in IoT.

Further investigation into the application of ABE (in particular, CP-ABE) to IoT is needed. This should be added to a knowledge base of findings such that a set of recommendations on device sizing against levels of computation and performance can be established. The recommendations should also consider architecture options such as proxy devices or assistant nodes to accommodate the heavier computation as well as act as security gateways to limit or prevent direct communication between the IoT device and the internet.

REFERENCES

[1] Sahai, A. and Waters, B. (2005). *Fuzzy identitybased encryption.* Springer. Advances in CryptologyEUROCRYPT 2005. pp. 457-473.

[2] Goyal, V., Pandey, C., Sahai, A. and Waters, B. (2006). *Attribute-based encryption for fine-grained access control of encrypted data*. ACM. Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89-98.

[3] Bethencourt, J., Sahai, A. and Waters, B., (2007) *Ciphertext-Policy Attribute-Based Encryption*. IEEE.
Proceedings of the IEEE Symposium on Security and Privacy, pp. 321-334

[4] Kumar, N., Rajya Lakshmi, G.V. and Balamurugan, B. (2015) *Survey of Attribute Based Encryption.* Elsevier. Procedia Computer Science Volume(46) pp. 689-696

[5] Qaio, Z., Liang, S., Davis, S. and Jiang, H. (2014) *Survey of Attribute Based Encryption.*IEEE. 15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing Proceedings of the IEEE Symposium on Security and Privacy, pp. 321-334

[6] Jin, Y., Tian, C., He, H. and Wang, F (2015) *A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing.* IEEE. 2015 IEEE Fifth International Conference on Big Data and Cloud Computing

[7] Hohenburger, S. and Waters, B.(2014) *"Online/offline attribute-based encryption," in Public-Key Cryptography* pp. 293-310

[8] Zhang, Y., Jin, L., Chen, X., Wong, D. and Li, H.(2013) *Anonymous attribute-based encryption supporting efficient decryption test* ACM Digital Library.Proceedings of the 8th ACM SIGSAC symposium on information, computer and communication security 2013

[9] Zhang, Y., Jin, L., Chen, X. and Li, H.(2016) *Anonymous attribute-based proxy re-encryption for access control in cloud computing* Wiley Online Library. Security and Communication Networks. 2016. Volume 9, Issue 14, pp. 2397-2411

[10] Chen, C., Zhang, Z. and Feng, D.(2011) *Efficiemt ciphertext-policy attribute-based encryption with constant cipher-text and constant computation-cost* Springer. Provable Security. pp. 84-101

[11] Zhang, Y., Zheng, D., Chen, J. Li, H.(2014) *Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts* Springer. Provable Security. pp. 259-273

[12] Guo, F., Susilo, W., Wong, D. and Varadharajan, V. (2014) *CP-ABE with Constant-Size Keys for Lightweight Devices* IEEE. IEEE Transactions on Information Forensics and Security, Vol 9, No. 5, pp. 763-771

[13] Odelu, V., Kumar Das, A., Sreenivasa Rao, Y., Kumari, S., Khan, M. and Choo, K. (2016) *Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment.* Elsevier. Computer Standards and Interfaces 2016

[14] Li, Q., Ma, J., Li, R., Xiong, J., Liu, X.(2015) *Provably secure unbounded multi-authority ciphertextpolicy attribute-based encryption* Wiley Online Library. Security and Communication Networks 2015. Volume 8, pp. 4098-4109

[15] Zhang, Y., Zheng, D., Li, Q., Jin, L. and Li, H.(2016) *Online/offline unbounded multi-authority attributebased encryption for data sharing in mobile cloud computing.* Wiley Online Library. Security and Communication Networks. 2016. Volume 9, Issue 16, pp. 3688-3702

[16] Yao, X., Chen, Z. and Tian, Y. (2015) *A lightweight attribute-based encryption scheme for the Internet of Things.* Elsevier. Future Generation Computer Systems
Volume 49 (2015) pp. 104-112

[17] Lee, J., Oh, S. and Jang, J.W. (2015) *A Work in Progress: Context based encryption scheme for Internet of Things.* Elsevier.Procedia Computer Science Volume(56) pp. 271-275

[18] Touati, L., Challal, Y. and Bouabdallah, A. (2014) *C-CP-ABE: Cooperative Ciphertext Policy AttributeBased Encryption for the Internet of Things.* 2014 International Conference on Advanced Networking Distributed Systems and Applications

[19] Touati L. and Challal, Y. (2015) *Batch-Based CPABE with Attribute Revocation Mechanism for the Internet of Things.* 2015 International Conference on Computing, Networking and Communications, Wireless Networks Symposium

[20] Touati L. and Challal, Y. (2015) *Efficient CP-ABE Attribute/Key Management for IoT Applications.* 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing

[21] Ambrosin, M. et al(2016) *On the Feasibility of Attribute-Based Encryption on Internet of Things Devices.* 2016 IEEE Micro Volume:36 Issue:6

[22] Ambrosin, M. et al(2015) *On the Feasibility of Attribute-Based Encryption on Smartphone Devices.* 2015 Proc.Workshop IoT Challenges in Mobile and Industrial Systems, pp49-54